Cellebrite
DIGITAL COLLECTOR

User Guide

May 2022 | Version 3.4

Cellebrite

This page intentionally left blank.

Preface

This user guide addresses only the most recent version of Cellebrite Inspector.

Legal Information

Typographic Conventions

This document uses these typographic conventions.

- The names of windows, views, tabs, dialog boxes, panes, panels, buttons, fields, options, checkboxes, and the like are in Initial Caps, or otherwise capitalized according to their labels.
- Keystrokes are shown in all capital letters, such as TAB, CTRL, OPT, CMD, SPACEBAR. Keys pressed at the same time are joined with +, such as CTRL+S, OPT+T.
- The names of elements that you are directed to interact with by clicking, selecting, or typing are shown in **bold**.
- Immediately contiguous menu actions such as clicking a toolbar button or menu, then immediately clicking another item in a resulting submenu, are separated with the > symbol, such as

  Edit > Copy
  Preferences > Data Collection

- *File names, folder names, file paths, disk names, drive names, volume names, partition names, and the like are shown in italic.* File extensions such as .pdf, .docx., .jpg, and so forth are not shown in italic.
- Variables are enclosed with <angle brackets>, such as <PLATFORM> VOLUMES, where <PLATFORM> is either MACOS or WINDOWS.
- `Anything you are directed to type exactly, such as file names, commands, or code, are shown in a console font.`

If you find any typos, inaccuracies, or other problems in this documentation, please send an email to support@cellebrite.com. Please include the title of the document, the version of the document, and the title of the topic in your message.

Contents

Document Revision History

This user guide addresses only the most recent version of Digital Collector.

This topic identifies information that is new, removed, or changed within this document for the 3.4 release of Digital Collector.

Description	Topic
This topic is new.	What's New in Version 3.4
Added and revised information throughout this manual regarding M1 Mac computers and macOS 11 and 12 to align with improvements discussed in the "What's New in 3.3" topic of the *Digital Collector 3.3 User Guide*.	These topics are new: • Imaging Considerations for macOS • Imaging M1 Mac Computers
Added information about custom file filters and collection templates, which were introduced in the "What's New in 3.3" topic of the *Digital Collector 3.3 User Guide*.	The Collection View topic was revised. The Templates menu was added to the Menu Bar topic. The Templates Menu topic is new. These topics are new or revised in the chapter titled "Collecting Data from a Source Computer": • Selecting User Files • Custom File Filters and Collection Templates • Create and Manage Custom File Filters • Collection Templates • Save Current Selections as a Template • Create and Manage Collection Templates • Apply a Collection Template
Ancillary to the changes required for custom file filters and collection templates, updated these topics.	• Selecting System Data • Selecting System Files • Selecting Additional Files and Folders

Description	Topic
Revised information about the *DCData* volume on the Digital Collector SSD. This aligns with the change from NTFS to exFAT discussed in the "What's New in 3.3" topic of the *Digital Collector 3.3 User Guide*. This includes the removal of the Other tab on the Preferences window because there is no longer an option to disable warnings about exFAT destination volumes.	• Digital Collector Device • Updating Digital Collector • Update Digital Collector on Mac Computers • Update Digital Collector on Windows Computers • Format Device Tool • Setting Preferences on a Mac Computer • Setting Preferences on a Windows Computer • Frequently Asked Questions
Revised information about previews to align with improvements discussed in the "What's New in 3.3" topic of the *Digital Collector 3.3 User Guide*.	• Browser View • Search View
Revised information about imaging for APFS volumes to align with improvements discussed in the "What's New in 3.3" topic of the *Digital Collector 3.3 User Guide*.	• Imaging Considerations for macOS • Launch Digital Collector on a Live Mac Computer • Acquire a Physical or Logical Image of a Mac Computer
To improve accuracy and visibility, revised the title of this topic and moved it to a different location in the Views section of the Workspace Orientation chapter.	Views of System Volume and Data Volume on Mac Computers
Added the Note paragraph.	Start a Windows Computer with Digital Collector
Added the Note paragraph to the description of the Content criteria.	Search View
Added information about the iCloud Drive message to Step 3.	Acquire a Physical or Logical Image of a Mac Computer
Added information about not writing to the *DCData* partition from a Windows computer started from the Digital Collector SSD when that partition is formatted NTFS.	Imaging Windows Computers
Identified the versions of macOS that SoftBlock can run on.	Preserving and Acquiring Digital Forensic Evidence
Added note and warning to not select the EFI partition.	Start a Mac Computer with Digital Collector

What's New in Version 3.4

These features and capabilities are new or changed in this release of Digital Collector.

Keyboard Navigation

The View menu provides new options for navigating among all the views in Digital Collector.

In addition, you can now use only a keyboard to navigate in Digital Collector. This is useful when a mouse is not available or not functioning. With normal keyboard navigation for your computer's operating system, you can perform all operations necessary to create an image or collect files. These keystrokes are particularly useful in Digital Collector.

Action	Mac	Windows
Open the next view (to the right)	CMD+TAB	CTRL+TAB
Open the previous view (to the left)	CMD+SHIFT+TAB	CTRL+SHIFT+TAB
Open a specific view or window	CMD+ 1 (Case Details) 2 (Browser) 3 (Search) 4 (Collection) 5 (Image) 6 (Mount Device) 7 (Format Device) 8 (Hash Device) 9 (Hash Image File) 0 (Terminal)	CTRL+ 1 (Case Details) 2 (Browser) 3 (Search) 4 (Collection) 5 (Image) 6 (Mount Device) 7 (Format Device) 8 (Hash Device) 9 (Hash Image File) 0 (Terminal)
Close window	CMD+W	CTRL+W
Switch among windows	CMD+`	ALT+TAB
Refresh device list	CMD+R	CTRL+R
Navigate among elements in the user interface (panes, fields, checkboxes, options, buttons)	TAB	TAB
Navigate among items in lists, menus	Arrow keys	Arrow keys
Make a selection, "press" a button	ENTER or SPACEBAR	ENTER or SPACEBAR
Open Menu bar	FN+CMD+F2	ALT+F or ALT+E
Close Digital Collector	CMD+Q	CTRL+Q

Preview Improvements for M1 Mac Computers

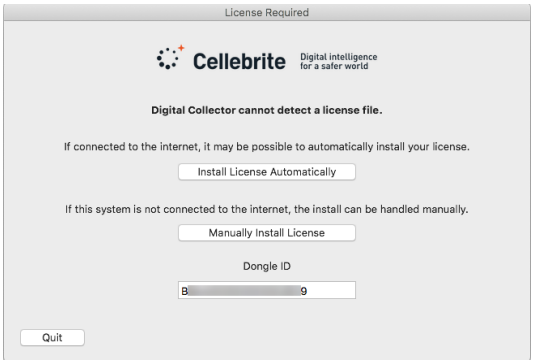
For M1 Mac computers booted from the Digital Collector SSD, improvements were made to file previews. File previews are now available for additional popular file types, including .rtf, .html, and MS Office files.

Improved Process to Install Renewed License

The process for installing your renewed Digital Collector license on your Digital Collector device (dongle) has been simplified. The License Manager application is no longer used. Instead, license installation is managed within Digital Collector itself or the updater app for Digital Collector.

Automatic

The easiest and recommended method is to run Digital Collector on a computer with an internet connection. If the license needs to be installed, the License Required dialog box automatically appears when you run Digital Collector.



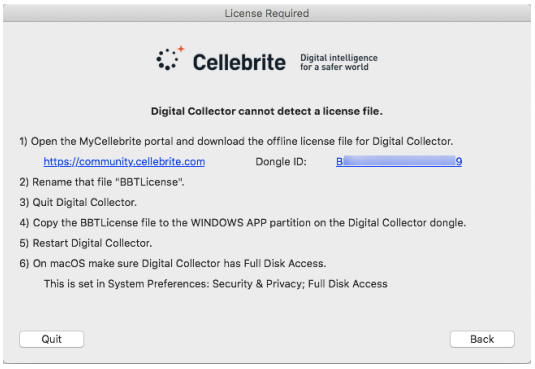
Click **Install License Automatically**.

Digital Collector automatically finds and installs your renewed license.

Manual

If automatic installation fails, click **Manually Install License**.

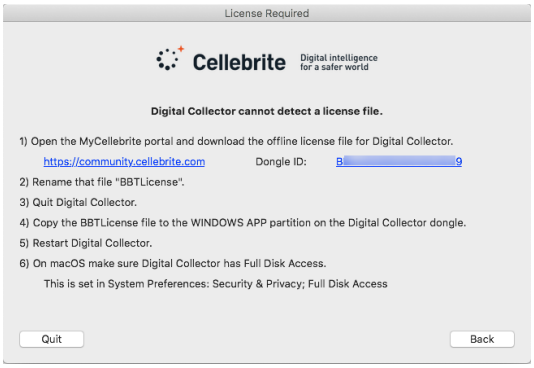
This License Required dialog box appears.



Follow the instructions to manually install the license.

Manual without Internet

If the computer running Digital Collector does not have an internet connection, click **Manually Install License**. This License Required dialog box appears.



1. Complete the first two steps on a separate computer that does have an internet connection and prepare to copy and paste the resulting file named *BBTLicense* with your usual method, such as by using a USB drive.
2. On the computer that the Digital Collector device is connected to, be sure that Digital Collector is not running.
3. Complete the remaining steps on the License Required dialog box.

Introduction

This user guide addresses only the most recent version of Cellebrite Digital Collector.

Cellebrite Digital Collector is a comprehensive software solution to help investigators collect and forensically image both static and live data from Mac and Windows computers as well as compatible external storage devices.

Digital Collector is designed for both novice and advanced users. It offers a clean interface featuring easy navigation as well as powerful advanced options. The interface provides forensic examiners both robust capabilities and an intuitive and elegant user experience throughout all phases of a digital forensic acquisition.

With Digital Collector, you can accomplish these tasks.

- Triage suspect computers and peripherals.
- Acquire data from live, running computers. (You can acquire RAM and volatile data only from Mac computers.)
- Select targeted data for collection.
- Create forensic images of computers and peripherals.

Digital Collector boots into a forensically sound environment on the Digital Collector device. You may also launch Digital Collector from your own analysis computer to acquire a connected device.

On Mac computers, you should launch Digital Collector from an administrator account when possible, so that it runs with admin-level permissions. When you launch with an administrator password, Digital Collector runs with root privileges.

This chapter provides these topics.

Intended Audience

Forensic software tools offered by Cellebrite are intended for use by law enforcement officials, private investigators, corporate security specialists, and other parties who investigate Mac-based and Windows-based computers devices for evidentiary data.

Users of Cellebrite software should possess these core competencies.

- Basic knowledge of and experience using Apple and Windows computers and their peripheral devices
- Familiarity with macOS and Windows operating system environments
- Knowledge and training in basic computer forensics policies and procedures
- An understanding of forensic images and how to correctly acquire them
- A fundamental understanding of how to preserve, acquire, authenticate, and analyze digital evidence, and how to report digital forensic investigation findings

Digital Forensics Overview

Forensics is preserving, acquiring, authenticating, analyzing, reporting, and managing digital evidence. Digital evidence includes data found on computer hard drives, external hard drives, CDs and DVDs, portable media such as USB thumb drives, Android devices, and iPod, iPhone, and iPad (iOS) devices.

A digital forensic examination includes these basic steps.

4. Preserve: Identify, secure, transport, and store the digital evidence (chain of custody).
5. Acquire: Create a forensically sound image of the evidence.
6. Authenticate: Confirm the forensic image is identical to the original (forensically sound).
7. Analyze: Create a case and analyze the evidence using an appropriate software solution.
8. Report: Thoroughly document the data investigation process and results of the analysis.
9. Manage: Back up, archive, detach/attach, and restore cases and evidence as needed.

Preserving and Acquiring Digital Forensic Evidence

Important: Protocol for preserving and acquiring digital evidence varies according to local, state, and federal laws, and according to corporate policy. Be aware of such protocol before you begin a digital forensic investigation.

Digital evidence must be preserved in its original form to the greatest extent possible for it to be admissible during a legal proceeding. A forensic examiner must carefully preserve, acquire, and authenticate electronic data during their examination. Therefore, it is of the utmost importance to acquire electronic evidence in a way that ensures no changes are made to the original data during the acquisition process.

A forensically sound image is a bit-by-bit image that is identical in every way to the original, including allocated, unallocated, and free space.

Preserving Evidence Using a Write-Blocker

Some operating systems attempt to write to the hard drive or device containing original evidence during the acquisition process. A write-blocker stands between the forensic examiner's computer or hardware acquisition tool and the devices containing the original evidence. Write-blockers prevent evidence contamination during the acquisition process.

Important: Always use a write-blocking hardware device or write-blocking software when acquiring digital evidence.

These are the types of write-blockers.

Hardware-Based Write-Blockers

A hardware-based write-blocker is a hardware device that is placed with cables and port connections between the forensic examiner's computer and the device containing the original digital evidence. Hardware-based write-blockers allow one-way, read-only data transfer between the device containing the evidence and the forensic examiner's computer. If the forensic examiner's operating system tries to write to the device containing the original data, the write-blocker blocks the unwanted data transfer.

Software-Based Write-Blockers

Software-based write-blockers serve the same purpose as hardware-based write-blockers. Software-based write-blockers reside on either the forensic examiner's computer, or on a hardware acquisition tool. SoftBlock™, offered by Cellebrite, is an example of a software-based write-blocker that runs on the forensic examiner's computer. (SoftBlock runs on computers running macOS 10.15 and earlier.) Digital Collector, offered by Cellebrite, is a hardware acquisition tool that has a software-based write-blocker built in.

A software-based write-blocker may be advantageous to a forensic examiner, as it may eliminate the need to purchase and carry expensive and cumbersome external hardware-based write-blockers.

Important: Be sure to test all write-blocking tools before performing an acquisition.

Note: For Mac computers, before you begin a forensic examination, you should also set .dmg files to read-only status as an additional safeguard. To do this, select the .dmg file(s), type COMMAND+L to open the Get Info window, and mark the **locked** checkbox.

Using SoftBlock During a Live Acquisition

A forensic examiner may need to acquire data from a machine while the machine is running, or live. Data collected during a live acquisition may be saved to a forensic image as needed. Live data may be acquired from hard drives or another electronic data source.

During a live acquisition, the device containing the original evidence must remain connected to the forensic examiner's machine throughout the investigation. A write-blocker must be in place throughout the investigation as well. SoftBlock is an excellent software-based write-blocking solution for live data acquisitions.

Acquiring Digital Evidence

A forensic image is a physical representation of the acquired device, even though it is saved as a file. Forensic images are static, meaning they remain the same even after you add them to a case. Forensic images may be backed up and stored for later use if necessary.

A forensic examiner uses these types of tools to acquire digital evidence.

Hardware Acquisition Tools: Hardware acquisition tools are physical devices used to collect digital evidence. They do not necessarily have a central processing unit (CPU), are self-contained, and may be hand-held. Digital Collector is an example of a hardware acquisition tool. Digital Collector can acquire a forensically sound image or collect data directly from a live source Mac or Windows computer (including RAM for macOS).

Software Acquisition Tools: Software acquisition tools reside on a forensic examiner's computer. Software acquisition tools often allow a forensic examiner to choose the forensic image file format, compression level, and the size of the data segments at the time the acquisition is performed. Inspector, offered by Cellebrite, has a software acquisition tool built in for acquiring iOS and Android devices.

Authentication and Hashing

After you acquire a forensic image, you must authenticate it to confirm the image is an exact copy of the original. This is accomplished by hashing both the source and the acquired image. Hashing is the process, done by forensic software, of applying an algorithm (mathematical formula) to generate a value that uniquely identifies data. This value is usually expressed as a sequence of hexadecimal digits. If the hash value of the acquired forensic image matches the hash value of the original data, the forensic image and original data can be considered identical.

Digital Collector and Inspector use these algorithms to generate hash values.

- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)
- Secure Hash Algorithm 2, 256-bit length (SHA-256)

Note: You may also hash individual files with Inspector.

Digital Collector Device

The same Cellebrite Digital Collector device works for both Windows and Mac computers. The solid-state drive (SSD) is either 120 GB or 1 TB and is shipped with two cables, USB 3.0 and USB-C. The SSD has several partitions, some of which may be hidden, and some of which you must not interact with.

Whether and how you see and interact with these partitions depends on if Digital Collector is running live or booted, if you're on a Mac or a Windows computer, and the manufacturer and BIOS for specific Windows computers.

Warning: When you connect Digital Collector to a running Windows computer, you may see prompts to format or scan drives. Always cancel these prompts! Windows interprets non-Windows file systems as drives that could be formatted, such as the *MacOS APP* partition that is formatted HFS Plus. Formatting any partitions on the Digital Collector SSD other than the *DCData* partition will require you to install Digital Collector on the SSD.

These are the partitions you may interact with.

Partition Name	Description
MacOS App	Contains the Digital Collector application to run on Mac computers. Also contains these files: • Digital Collector EULA.txt • Digital Collector 3rd Party Licenses.txt
WINDOWS APP	Contains the Digital Collector application to run on Windows computers. Also contains these files: • Digital Collector EULA.txt • Digital Collector 3rd Party Licenses.txt • Digital Collector license file • com.cellebrite.DigitalCollector.settings
DCData	A storage partition formatted with exFAT. This best supports reading images on both the Mac and Windows platforms. (Cellebrite had previously discouraged exFAT because older versions of macOS had some problems with their exFAT implementations. In recent years those issues seem to have been fixed. If you do encounter issues, you can change the format of the *DCData* partition.) The *DCData* partition can be used as a destination drive during quick, smaller data collections. The size of the *DCData* partition is larger on the 1 TB SSD than on the 120 GB SSD. There are two ways to make space in the *DCData* partition for new collections. • Delete files within the partition using any computer that supports exFAT. • Use the Format Drive tool within Digital Collector to delete all the contents of the partition.

There are also partitions you can use when you need to start (boot) Mac computers running operating systems older than macOS Sierra 10.12.

Note: If you intend for the *DCData* partition to be used as a destination for a folder-based collection (not an L01-based collection, Sparseimage-based collection, or disk image) from a Mac computer, you should reformat the *DCData* partition to APFS or HFS Plus using the Format Drive tool within Digital Collector. The name of this partition must always be *DCData*. For more information, see Format Device Tool.

If the collection is larger than the space available on the *DCData* partition, you must use an external storage device to serve as the destination. For more information, see Other Equipment.

Operating Systems

A single Digital Collector solid state drive (SSD) can run on both the Mac and Windows platforms.

Digital Collector will run on live Windows computers with 64-bit hardware running Windows 10, version 1909 and newer. It will start (forensically boot) Windows computers running Windows 10 and may start older Windows operating systems.

Digital Collector can run on live Mac computers and also start (forensically boot) Mac computers with these operating systems:

- macOS Monterey 12
- macOS Big Sur 11
- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12

Additional (legacy) boot partitions let you attempt to start Mac computers with operating systems including OS X El Capitan 10.11 and older. If a Mac computer cannot boot to the current version of Digital Collector, try again with the first additional boot partition. If necessary, attempt again with the remaining boot partitions in ascending numerical order.

Warning: Cellebrite cannot ensure that Digital Collector will run properly on early versions of any macOS, such as 12.0. or 12.1. Support is generally declared by the time later versions are released, such as 12.3.

There are some constraints to be aware of in specific circumstance. For more information, see Imaging Considerations for macOS.

File Systems and Decryption

Cellebrite Digital Collector supports decryption in these scenarios when you provide the correct credentials.

Windows Computers

Digital Collector can acquire an image of an encrypted disk on Windows. Digital Collector cannot decrypt data during imaging or unlock encrypted disks for data collection from Windows computers.

If the encryption is a variant supported by Inspector, such as BitLocker, the image can be decrypted during ingestion.

Mac Computers

Digital Collector supports decryption during imaging or for data collection from Mac computers using software or hardware encryption.

Software encryption:

- CoreStorage (HFS Plus) with FileVault 2
- APFS with FileVault 2

Hardware-assisted encryption:

- M1 chip
- T2 chip

There are some constraints to be aware of in specific circumstance. For more information, see Imaging Considerations for macOS.

Other Equipment

You should be prepared to use Cellebrite Digital Collector under any circumstance and have other necessary equipment immediately available.

The Digital Collector solid state drive (SSD) ships with a USB 3.0 cable and a USB-C cable. You will encounter a variety of Mac and Windows computers with different amounts and types of ports. The cables and types of connections required to connect source computers to your host computer depend on the platforms, the manufacturers, and the models.

Therefore, you should equip yourself with an assortment of high-quality cables, adapters, and powered hubs to ensure that you can provide power to devices and can properly connect devices to each other.

Before you connect a source computer to a host or analysis computer, you must have write blocking in place. This can be either a hardware-based write-blocker or a software-based write-blocking application that you install on your own host computer. Cellebrite offers SoftBlock™, which lets you choose to mount newly attached computers and hardware devices with read-only or read-write permissions. SoftBlock runs on computers running macOS 10.15 and earlier. (Hardware write blockers add a layer of complexity. The hardware write blocker must be considered when determining the cables and adapters required. If there are difficulties, the hardware write blocker itself as well as its connections present additional items for troubleshooting.)

The *DCData* volume on the Digital Collector SSD may not have enough available space to hold large images or data collections. Therefore, you should also have on hand external hard drives or SSDs in appropriate formats with sufficient capacity to serve as the destination.

For starting (booting) source computers with Digital Collector, you should have wired keyboards that can connect to various Mac and Windows computers. This is because a wireless keyboard may not transmit keystrokes to the source computer in time to prevent it from booting to its internal operating system.

Considerations for Mac Computers

When you work with Mac hardware, genuine Apple cables and adapters are required. Off brand cables and adapters are not sufficiently reliable and capable.

Target disk mode (TDM) is a Mac feature that essentially turns the computer into an external hard drive. The original purpose of TDM was file transfer. When you place a source computer in TDM, you can create an image of it with Digital Collector. When a source Mac computer is in TDM it will be written to when connected to another computer, which means write blocking is required.

Older Mac computers require a FireWire connection to use the TDM interface. Newer Mac computers allow access with Thunderbolt and USB. For more information, see https://support.apple.com/en-us/HT201462. In particular, the Apple USB-C TB3 cable is the most reliable for connecting a host computer with a USB-C port to a source computer in TDM. If the host computer has a Thunderbolt 2 port, the most reliable connection is the Apple TB cable and Apple TB3 to TB2 adapter.

Note: TDM does not exist on M1 Mac computers.

Product Registration

Cellebrite Digital Collector product license registration occurs at the time of purchase and before the product is shipped. Each license is bound to a Digital Collector device.

Subscriptions

Each new Digital Collector product purchase includes a one-year license subscription. During this one-year subscription period, you have the right to download and install all Digital Collector updates and new releases.

Please be sure to renew your product license subscriptions annually through your Cellebrite Sales Representative to continue receiving subscription benefits.

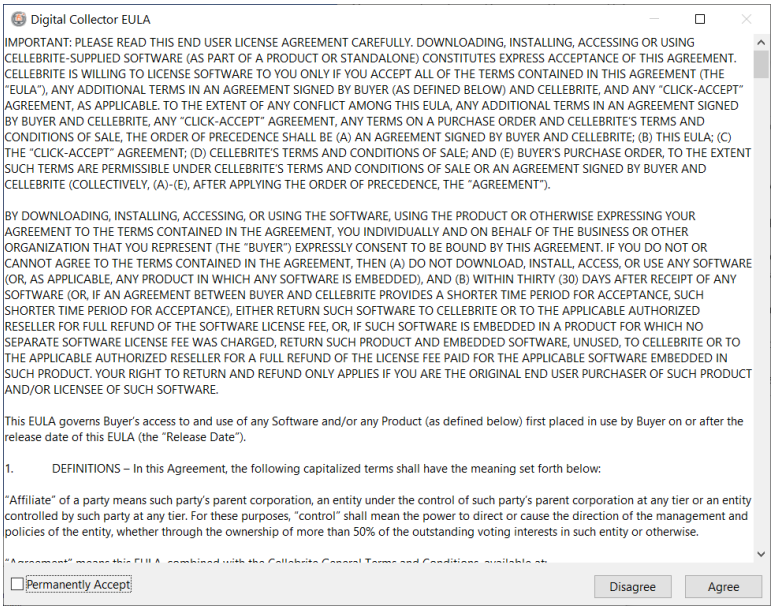
You may view your current registration information, check for product updates, and download new product releases. For more information, see Getting Support.

Accepting the Digital Collector End User License Agreement

To accept the End User License Agreement (EULA), you must launch Cellebrite Digital Collector. You can do this on any computer you wish, but it is most practical to do this on your own computer as soon as you receive the Digital Collector device. This topic assumes that you are using your own computer to accept the EULA, rather than a source computer, and that you have administrator credentials.

Permanently Accept the EULA on a Windows Computer

1. Connect the Digital Collector SSD to a USB port on the computer.
   Ignore any prompts to scan or format the SSD.
2. Use File Explorer see the *WINDOWS APP* partition.
3. In the *WINDOWS APP* partition, double-click **DigitalCollector.exe**.
4. Choose the appropriate action.
   - If User Account Control (UAC) is not enabled, go to Step 5.
   - If User Account Control (UAC) is enabled and the logged-in user:
     - has administrative permissions, click **Yes**. The Digital Collector End User License Agreement (EULA) window appears.
     - does not have administrative permissions, enter an administrator password, clicking **More Choices** if necessary to see all the user accounts for this computer. The Digital Collector End User License Agreement (EULA) window appears.



5. In the lower left corner of the Digital Collector EULA window, mark the **Permanently Accept** checkbox, and then click **Agree**.
   The Digital Collector window appears.

Permanently Accept the EULA on a Mac Computer

1. Connect the Digital Collector SSD to a USB port on the computer.
2. Use Finder to browse to the *MacOS App* partition on the SSD, and then double-click **DigitalCollector.app**.
3. Provide login credentials for your administrative user account.
4. Type your credentials in the **User Name** and **Password** fields, and then click **Install Helper**.
   The Digital Collector End User License Agreement (EULA) window appears.
5. In the lower left corner of the Digital Collector EULA window, mark the **Permanently Accept** checkbox, and then click **Agree**.
   The Digital Collector window appears.

Updating Digital Collector

Cellebrite Digital Collector solid state drives (SSD) ship with the most recent Digital Collector software version. Nonetheless, you should check for software updates the first time the software is launched, and periodically thereafter to ensure the software remains up to date. The Check for Updates feature requires an active Internet connection.

You can update the Digital Collector SSD on either a Mac or a Windows computer.

- Update Digital Collector on Mac Computers
- Update Digital Collector on Windows Computers
- Troubleshooting the Cellebrite Digital Collector Updater

As of version 3.3, the Digital Collector updater app formats the *DCData* partition as exFAT.

The updater app runs on these operating systems:

- macOS 10.14.3 and newer
- Windows 10 only, v 1909 or newer

Receive Product Announcements

The Cellebrite Customer Support team sends product update notices by email to customers who choose to receive future product announcements. These notices often include a direct download link for the latest software version.

To receive Digital Collector product update notices by email, please send an email to support@cellebrite.com. The subject line must be "Cellebrite Digital Collector Product Information Opt-in Request". Also include your name (or organization name) and additional contact information in the email body.

Update Digital Collector on Mac Computers

You must check for updates and then download the updater before you run the update process for the Cellebrite Digital Collector solid state drive (SSD). As of version 3.3, the Digital Collector updater app formats the *DCData* partition as exFAT.

Check for Updates

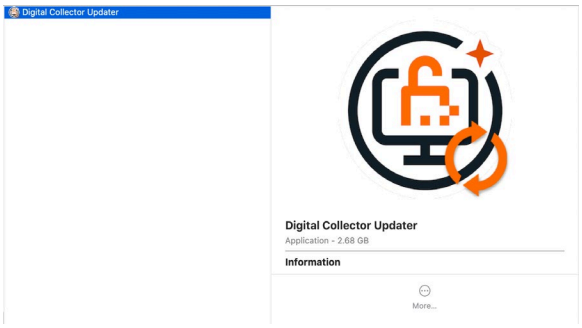
1. In the Digital Collector menu bar, click **Digital Collector > Check for Updates**.
2. Log in to the Cellebrite Customer Community.
3. If a newer Digital Collector software version is available, the Software Update window shows this message: `An Update was found`.
4. Choose one of these actions.
   - To skip the update and dismiss the Software Update window, click **Skip This Version**.
   - To temporarily dismiss the Software Update window, click **Remind Me Later**.
   - To download the Digital Collector Updater, click **Download Update** and follow the prompts.

Update Digital Collector

You must update the Digital Collector SSD to update the Digital Collector software.

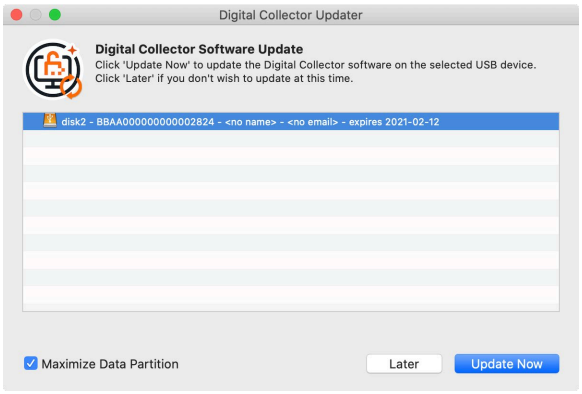
Warning: Do not disconnect the Digital Collector SSD from the computer until the update process is complete. Doing so may render the device unusable.

1. After you check for updates and download the Digital Collector Updater archive file, extract the update from the archive.
2. Select the extracted folder. The Digital Collector Updater window appears.



3. Double-click the Digital Collector Updater icon, and then provide administrator credentials to allow the updater to run with root privileges.
4. Click **Install Helper**.
   If more than one USB device is detected on the computer, you see a message confirming that only the active Digital Collector SSD is listed in the updater device list.

5. The Digital Collector Updater window appears, and the Digital Collector SSD is automatically selected in the Digital Collector Updater window.



6. Click **Update Now** to begin the update process.

Update Digital Collector on Windows Computers

You must first check for and then download the updater before you run the update process for the Cellebrite Digital Collector solid state drive (SSD). As of version 3.3, the Digital Collector updater app formats the *DCData* partition as exFAT.

Check for Updates

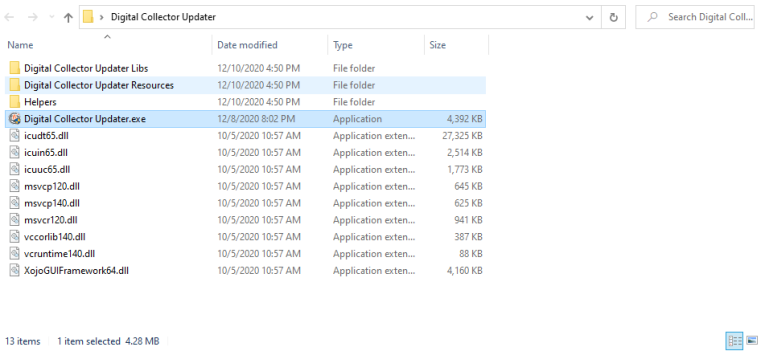
1. In the Digital Collector menu bar, click **Help > Check for Updates**.
2. Log in to the Cellebrite Customer Community.
3. If a newer Digital Collector software version is available, the Software Update window shows this message: An Update was found.
4. Choose one of these actions.
    - To skip the update and dismiss the Software Update window, click **Skip This Version**.
    - To temporarily dismiss the Software Update window, click **Remind Me Later**.
    - To download the Digital Collector Updater, click **Download Update** and follow the prompts.

Update Digital Collector

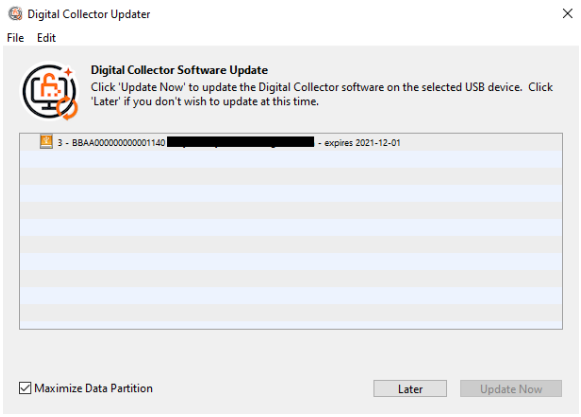
You must update the Digital Collector SSD to update the Digital Collector software.

Warning: Do not disconnect the Digital Collector SSD from the computer until the update process is complete. Doing so may render the device unusable.

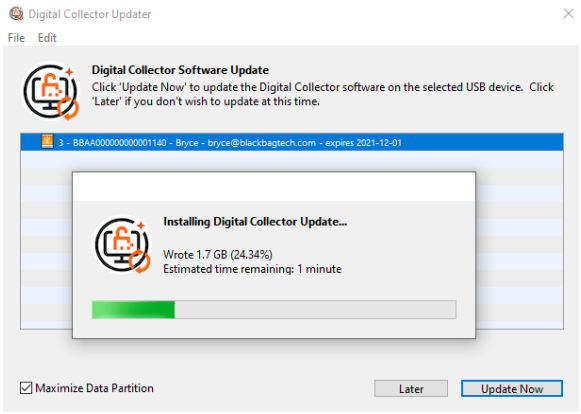
1. After you check for updates and download the Digital Collector Updater archive file, extract files from the archive.



2. In the extracted Digital Collector Updater folder, double-click **Digital Collector Updater.exe**. The Digital Collector Updater window appears.



3. Click **Update Now**.
The update for Digital Collector is installed.



Troubleshooting the Cellebrite Digital Collector Updater

With the help of these topics, you may be able to troubleshoot these specific issues yourself. If you experience difficulties during the update process, contact support@cellebrite.com.

Digital Collector Mounted with Read-only Permissions

The Digital Collector SSD may mount with read-only permissions on computers with SoftBlock™ installed if the Digital Collector device was attached to the computer when it was started or restarted.

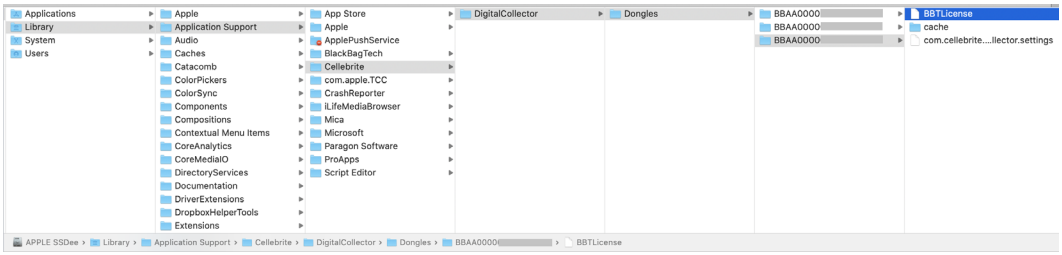
If the Digital Collector SSD mounts with read-only permissions, the Digital Collector Updater window shows this text in red: [READ ONLY].

Unmount the Digital Collector SSD and remount it with Read-Write permissions. The Digital Collector Updater should then run normally. For more information, see Mount Device Tool.

License File Restore Error

If the Digital Collector Updater fails to restore the license file to the Digital Collector SSD, you can manually restore the license file from its backup.

1. To find a Digital Collector license file backup, click **Reveal License File**.
   This file has this extension: .BBTLicense
   - On a Mac computer, a Finder window opens and displays the license backup file.



   - On a Windows computer, a File Explorer window opens and displays the license backup file.

2. Drag and drop the backup file to the mounted Digital Collector device into the *WINDOWS APP* partition.

Getting Support

Before you contact technical support or your Sales Representative, you must get the ID for your Digital Collector SSD from the Preferences window. For more information, see Getting Information About a Digital Collector Device.

You can log in to your account in the MyCellebrite portal at https://community.cellebrite.com, which provides access to resources and support.

- Keep your products updated.
- Contact Support or review the knowledgebase.
- Download user manuals and data sheets.
- Manage your product licenses.
- Get expert assistance.

You can also send an email to technical support at support@cellebrite.com.

These technical publications are available for download.

- *Cellebrite Digital Collector Release Notes*
- *Cellebrite Digital Collector Quick Start Guide*
- *Cellebrite Digital Collector User Guide*

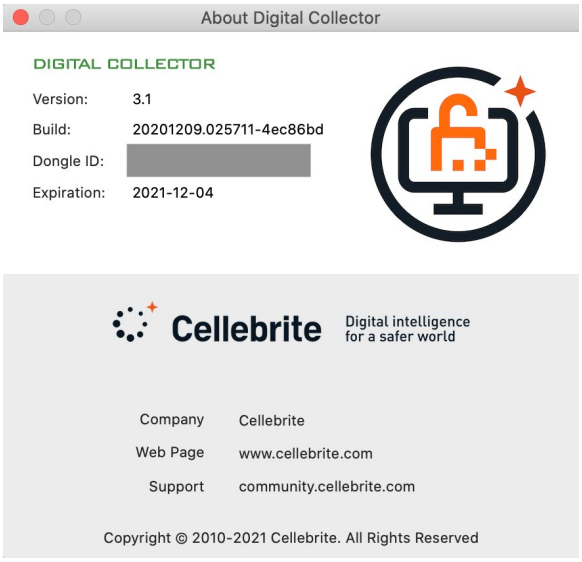
Getting Information About a Digital Collector Device

On the About Digital Collector window, you can find this information about your Cellebrite Digital Collector solid state drive (SSD).

Version	The version of Cellebrite Digital Collector on this SSD
Build	The specific build identification number for this version of Digital Collector
Dongle ID	The identification number for this Digital Collector SSD You must have this ID before you contact Technical Support.
Expiration	The date when the license subscription contract expires. Digital Collector stops functioning after the subscription expires.

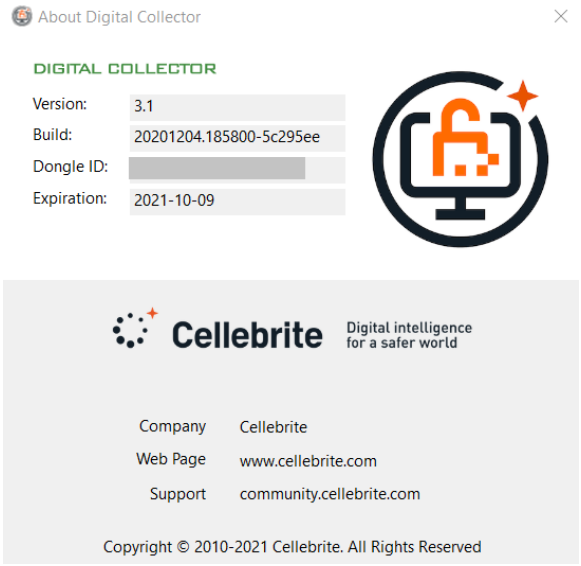
Open the About Digital Collector Window on a Mac Computer

In the menu bar, click **Digital Collector > About Digital Collector**.



Open the About Digital Collector Window on a Windows Computer

In the menu bar, click **Help > About Digital Collector**.



Workspace Orientation

You should understand these main parts and capabilities of the Digital Collector interface.

- Menu Bar
- Toolbar
- Views
- Refresh the Device List
- Setting Preferences on a Mac Computer
- Setting Preferences on a Windows Computer

Menu Bar

The menu bar in Cellebrite Digital Collector is located at the top of the screen on a Mac computer and at the top of the application window on a Windows computer. The menu bar has these options.

Option	Mac	Windows	Topic
Digital Collector	✓		Digital Collector Menu
File	✓	✓	File Menu
Edit	✓	✓	Edit Menu
Action	✓	✓	Action Menu
Templates	✓	✓	Templates Menu
Window	✓	✓	Window Menu
Help	✓	✓	Help Menu

Digital Collector Menu

The Digital Collector menu is available only on Mac computers.

In the menu bar, click **Digital Collector**, and then click the appropriate action.

Option	Description
About	Version, device ID, license expiration, and contact information for Digital Collector. For more information, see these topics: • Getting Support • Getting Information About a Digital Collector Device
Check for Updates	Check to see if there is a newer version of Digital Collector. For more information, see Updating Digital Collector.
Preferences	Open the Digital Collector Preferences dialog box. For more information, see Setting Preferences on a Mac Computer.
Hide Digital Collector	Hide Digital Collector.
Hide Others	Hide all applications except Digital Collector.
Quit Digital Collector	Stop and exit Digital Collector.

File Menu

In the menu bar, click **File** and then click the appropriate option.

Option	Description	Mac	Windows
Close	Close the current window.	✓	✓
Refresh Device List	Force the device list to refresh. For more information, see Refresh the Device List.	✓	✓
Exit	Stop and exit Digital Collector.		✓

Edit Menu

In the menu bar, click **Edit** and then click the appropriate option.

Option	Description	Mac	Windows
Undo	Undo the previous action.	✓	✓
Cut	Cut the current selection.	✓	✓
Copy	Copy the current selection.	✓	✓
Paste	Paste the selection previously cut or copied.	✓	✓
Delete	Delete the current selection.	✓	✓
Select All	Select all items.	✓	✓
Deselect All	Deselect all items.	✓	✓
Preferences	Open the Digital Collector Preferences dialog box. For more information, see Setting Preferences on a Windows Computer.		✓

Action Menu

In the menu bar, click **Action** and then click the appropriate option.

Option	Description	Mac	Windows
Add selected items to collection	Add the currently selected item or items to the collection. The Action menu is active only on the Browser and Search views in Digital Collector.	✓	✓

Templates Menu

In the Menu bar, click **Templates** and then click the appropriate option.

Option	Description	Mac	Windows
Apply Collection Template	Select collection templates to apply for collecting data from the source computer. For more information, see Apply a Collection Template.	✓	✓
Configure Collection Templates	Create, change, and delete collection templates. For more information, see Create and Manage Collection Templates.	✓	✓
Save Current Selections As Template	Save the current selections on the Collection view as a collection template. For more information, see Save Current Selections as Template.	✓	✓
Configure Custom File Filters	Create and manage custom file filters to use when selecting items to collect. For more information, see Create and Manage Custom File Filters.	✓	✓

For more information, see Custom File Filters and Collection Templates.

Window Menu

In the menu bar, click **Window** and then click the appropriate option.

Option	Description	Mac	Windows
Activity	Opens the Activity window. For more information, see Activity Window.	✓	✓

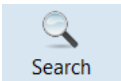
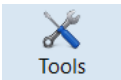
Help Menu

In the menu bar, click **Help**, and then click the appropriate option.

Option	Description	Mac	Windows
User Guide	Open the User Guide for Cellebrite Digital Collector.	✓	✓
Cellebrite Website	Open the Cellebrite homepage in a web browser.	✓	✓
Digital Collector Feedback	Provide feedback to Cellebrite via email.	✓	✓
Technical Support	Open the Cellebrite website technical support page in a web browser.	✓	✓
About Digital Collector	Version, device ID, license expiration, and contact information for Digital Collector. For more information, see these topics: • Getting Support • Getting Information About a Digital Collector Device		✓
Check for Updates	Check to see if there is a newer version of Digital Collector. For more information, see Updating Digital Collector.		✓

Toolbar

The toolbar lets you open views in Cellebrite Digital Collector.

Button	Description
	Opens the Case Details view, where you can provide information to identify a case and the examiner. You can also adjust the date and time zone of timestamps for acquisition log files and reporting purposes. Source data (potential evidence) is not modified.
	Opens the Browser view, where you can navigate through the file systems of the connected devices.
	Opens the Search view, where you can use robust tools to determine whether a connected device contains information of interest.
	Opens the Collection view, where you can strategically acquire targeted files, folders, and system data from a source device, rather than creating a full bit-by-bit forensic image.
	Opens the Image view, where you can acquire a bit-by-bit forensic image of a device, or image a partition or slice.
	Opens the Tools view, where you can use a set of tools useful for advanced forensic examiners.

Views

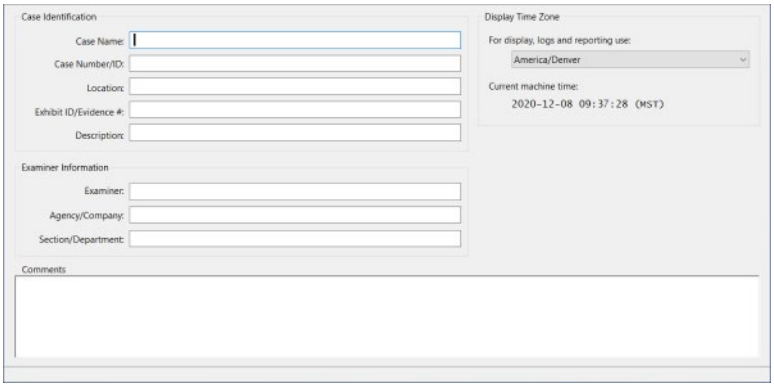
These are the views in Cellebrite Digital Collector.

- Case Details View
- Browser View
- Search View
- Collection View
- Image View
- Views of System Volume and Data Volume on Mac Computers
- Tools View

Case Details View

The Case Details view lets you manage information about the case and the examiner.

On the Cellebrite Digital Collector toolbar, click **Case Details**. The Case Details view appears.



On the left side of the Case Details view, type the necessary information in the fields for Case Identification and Examiner Information.

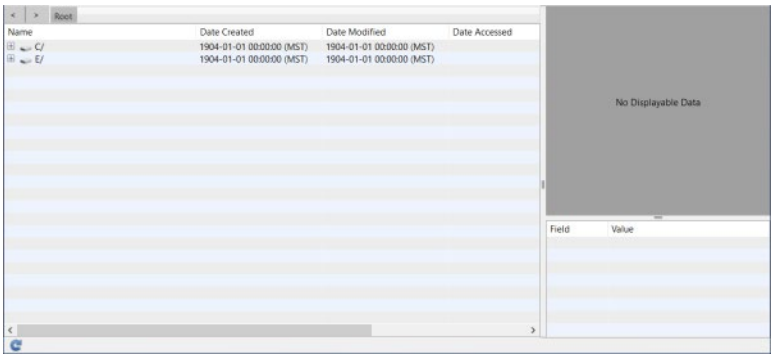
In the **Comments** field, type any additional information about the acquisition.

By default, acquisition log files record date and timestamps according to the host or analysis machine's system date and time settings. To adjust the display time zone, select the appropriate time zone. This is strictly for logging and reporting purposes. Source data (potential evidence) is not modified.

Browser View

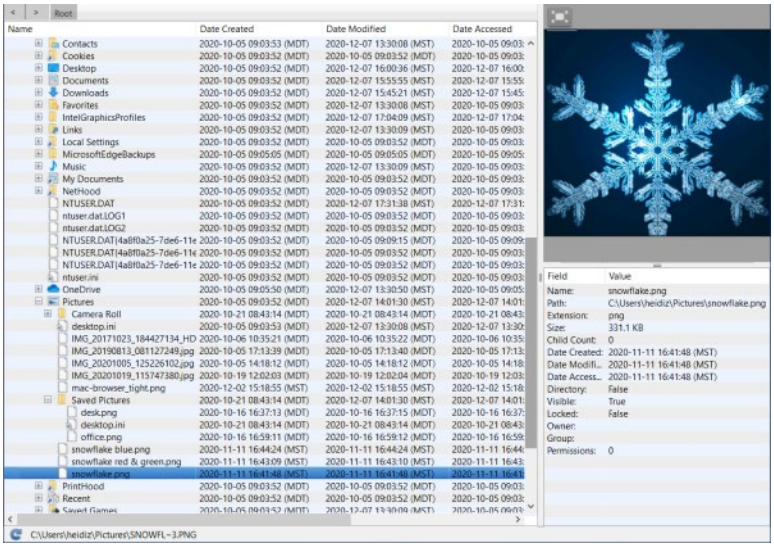
The Browser view in Cellebrite Digital Collector allows you to navigate through the file systems of connected devices. You can also select files and folders and add them to the set of data to be collected.

In the toolbar, click **Browser** to see the connected volumes.



In the Browser view, you can navigate through the directory structure of connected devices. When you select a file, a preview appears on the right side along with file metadata.

Note: Using the Browser view in live mode to preview contents of connected source volumes results in changes to the file system. For more information, see Appendix: Changes to Live Computers.



On Mac computers, you can see file previews for file types supported by QuickLook, such as pictures, videos, MS office files, .pdfs, and more.

Note: For M1 Mac computers, previews for MS Office files are only available from live, running computers. They are not available for M1 Mac computers started (booted) from Digital Collector.

On Windows computers, you can see file previews for image file types, such as .jpg, .png, .gif, and more. You can also see previews for MS Office files.

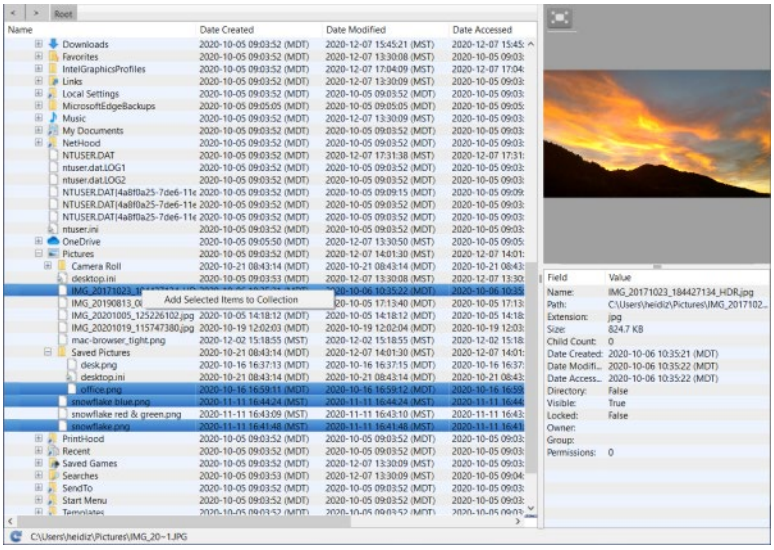
For image files only, above the preview pane you can toggle between viewing scaled to fit the preview pane or viewing full sized.

On Mac computers with FileVault 2, the encrypted volume is already unlocked if the computer is running. If the computer is not running, you must first mount it and then unlock the FileVault 2 encrypted volume with a user account password, a recovery key, or keychain file if you are an Enterprise user. For more information, see Mount Device Tool and Unlocking and Imaging CoreStorage FileVault 2 Volumes.

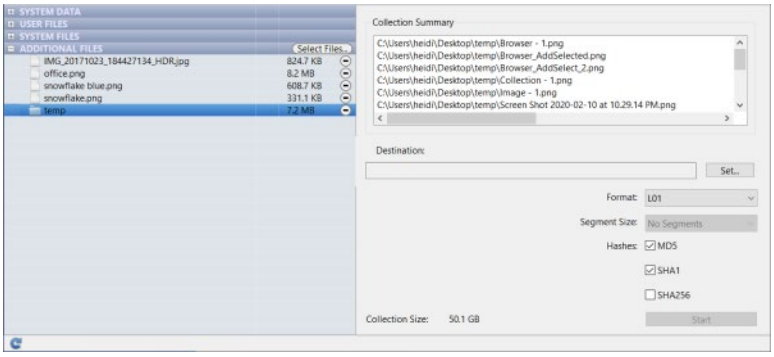
If you are examining a computer running on macOS 10.15 or later, see Views of System Volume and Data Volume on Mac Computers.

Adding Files to the Collection

From the Browser view, you can add files and folders to the set of data to be collected. You can add files and folders one at a time or in groups. Use normal operating system procedures to select files and folders individually or sequentially, then open the context menu (right-click a selected item) and click **Add Selected Items to Collection**.



Files added to the collection this way appear in the ADDITIONAL FILES section of the list on the Collection view. For added folders, the contents of the folder are listed in Collection Summary when a folder is selected in the ADDITIONAL FILES section.

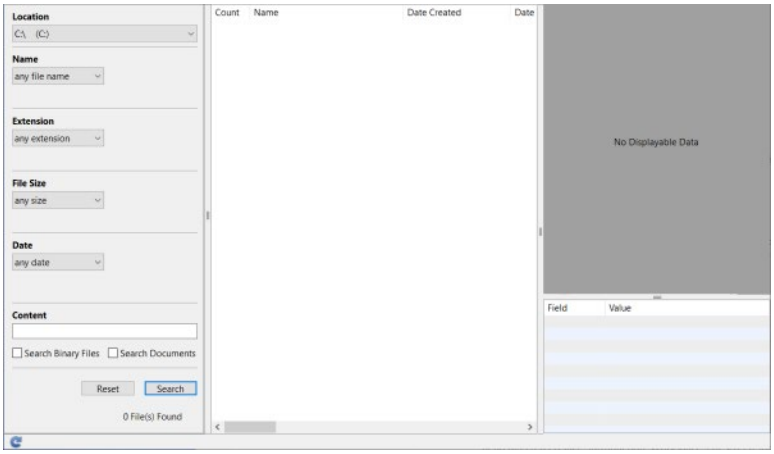


For more information, see Selecting Additional Files and Folders.

Search View

You can use the Search view in Cellebrite Digital Collector to determine whether a connected device contains information of interest. If no items are returned from searches, further processing of the device may not be necessary.

In the toolbar, click **Search**.



The Search view allows you to search for data based one or more of these criteria.

- Location - Volume or specific path
- Name - Filename using these operators
  - contains
  - does not contain
  - exact match
- Extension - File extension using these operators
  - is
  - is not
- File Size - File size using these operators. You can specify the file size to search for in KB, MB, or GB.
  - greater than
  - less than
  - between
- Date - Choose Date Created, Date Modified, or Date Accessed, then choose an operator and set the dates be typing, using the arrows, or selecting from the calendar.
  - is between
  - is before
  - is after
  - is exactly
- Content - Search for files containing content you specify. You can search data within binary files, documents, or both. If both binary files and documents are selected, the search time increases, sometimes significantly.

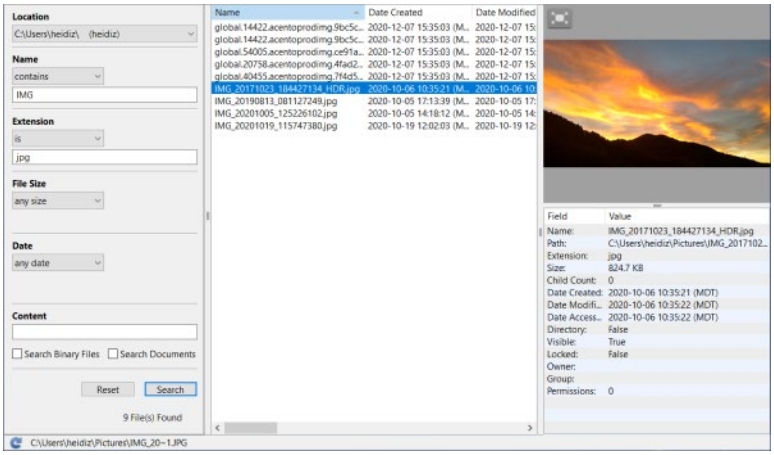
Note: Files containing UTF-8 international characters do not appear in results when using the Search view with the Content criteria.

You can combine multiple search criteria to create a more complex search, filtering down to items that are relevant to the investigation.

Reviewing Results

When you select a file from the search results, a preview appears on the right side along with file metadata.

Note: Using the Search view in live mode to preview contents of connected volumes results in changes. For more information, see Appendix: Changes to Live Computers.



For image files only, above the preview pane you can toggle between viewing scaled to fit the preview pane or viewing full sized.

On Windows computers running live, you can see file previews for image file types, such as .jpg, .png, .gif, and more. You can also see previews for MS Office files.

On Mac computers, you can see file previews for file types supported by QuickLook, such as pictures, videos, MS office files, .pdfs, and more.

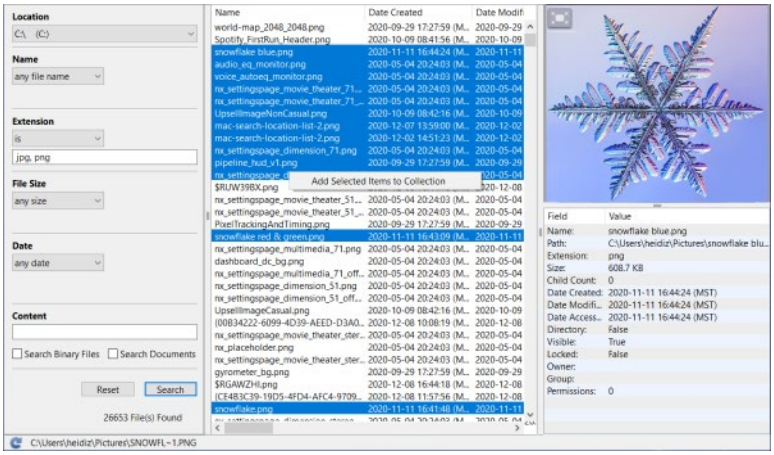
Note: For M1 Mac computers, previews for MS Office files are only available from live, running computers. They are not available for M1 Mac computers started (booted) from Digital Collector.

On Mac computers with FileVault 2, the encrypted volume is already unlocked if the computer is running. If the computer is not running, you must first mount it and then unlock the FileVault 2 encrypted volume with a user account password, a recovery key, or keychain file if you are an Enterprise user. For more information, see Mount Device Tool and Unlocking and Imaging CoreStorage FileVault 2 Volumes.

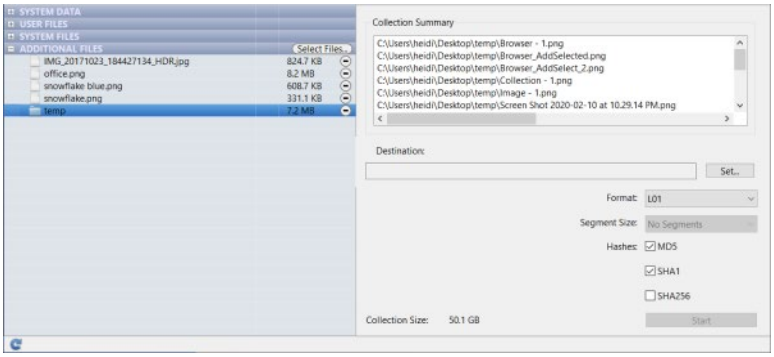
If you are examining a computer running on macOS 10.15 or later, see Views of System Volume and Data Volume on Mac Computers.

Adding Files to the Collection

From the Search view, you can add files and folders to the set of data to be collected. You can add files and folders one at a time or in groups. Use normal operating system procedures to select files and folders individually or sequentially, then open the context menu (right-click a selected item) and click **Add Selected Items to Collection**.



Files added to the collection this way appear in the ADDITIONAL FILES section of the list on the Collection view. For added folders, the contents of the folder are listed in Collection Summary when a folder is selected in the ADDITIONAL FILES section.



For more information, see Selecting Additional Files and Folders.

Collection View

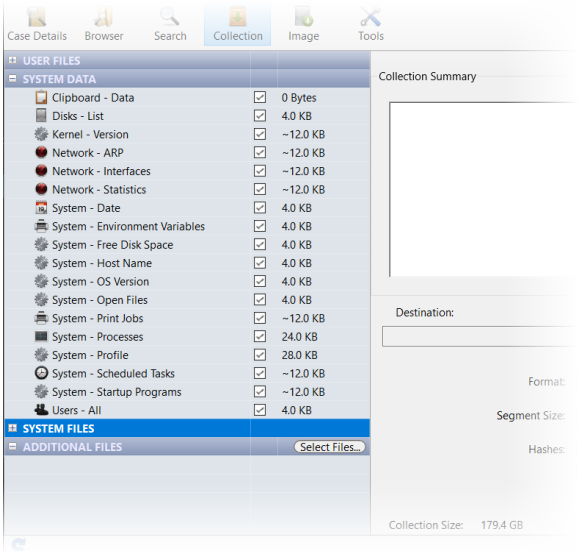
The Collection view in Cellebrite Digital Collector allows you to acquire selected files, folders, and system data from a source computer or any drive or storage device attached to it. With this powerful feature, you can strategically triage data instead of creating a full bit-by-bit forensic image when time is short or other external constraints are present.

The Collection view automatically targets these data categories:

- User Files
- System Data
- System Files
- Additional Files

You can also create and use custom file filters and collection templates, which make it easier and faster to select items to collect. For more information, see Custom File Filters and Collection Templates.

To see the Collection view, click **Collection** in the toolbar.



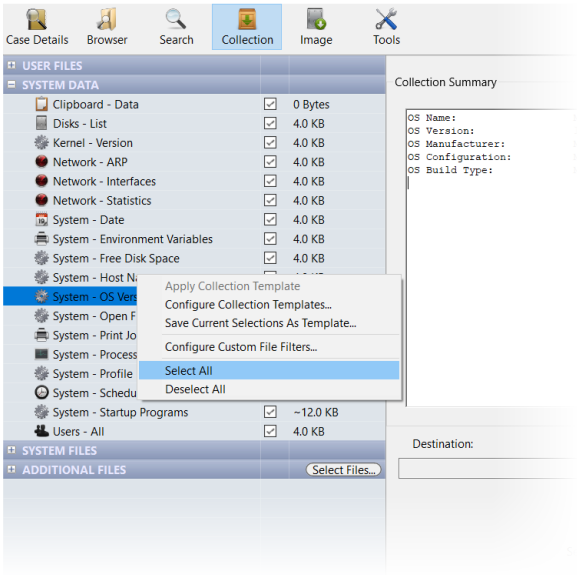
If you are examining a computer running on macOS 10.15 or later, see Views of System Volume and Data Volume on Mac Computers.

You can expand each category in the list to see the targeted data. Mark the checkbox to the right of any items to select them for collection.

You can select or deselect all items within a category of the list, for example all user directories within the USER FILES category.

- On a Mac computer, press OPTION while clicking a checkbox for one item within the category.
- On a Windows computer, press ALT while clicking a checkbox for one item within the category.

To select or deselect every item in all categories, open the context menu (right-click any item) and then click **Select All** or **Deselect All**.



You can add files and folders to the ADDITIONAL FILES section of the list. Click **Select Files** to the right of ADDITIONAL FILES, and then navigate to the files and folders that should be added to the collection.

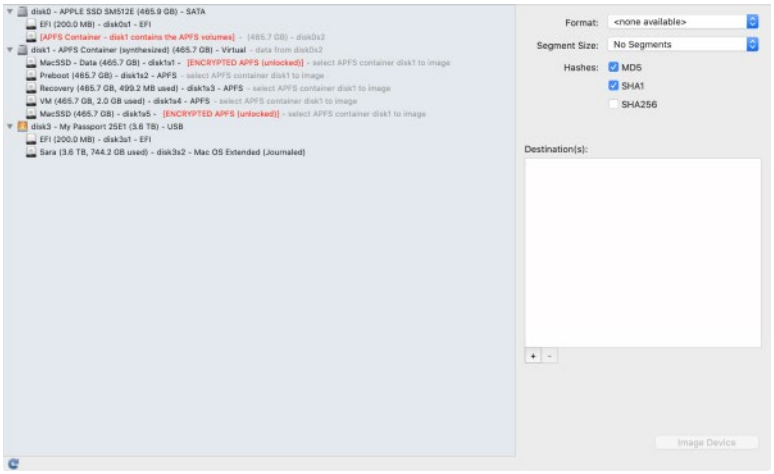
You can also add files and folders to the collection directly from the Browser and Search views. For more information, see Browser View and Search View.

Image View

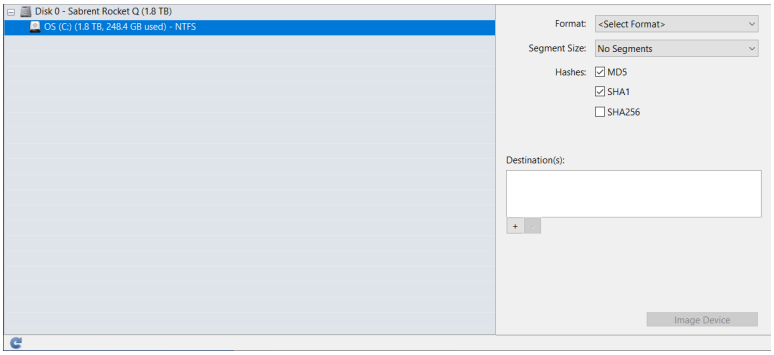
The Image view in Cellebrite Digital Collector lets you easily acquire a bit-by-bit forensic image of a computer hard drive or an attached external storage device, or to image a device partition or slice.

In the Digital Collector toolbar, click **Image**.

This is an example of the Image view on a Mac computer. If you are examining a computer running on macOS 10.15 or later, see Views of System Volume and Data Volume on Mac Computers.



This is an example of the Image view on a Windows computer.

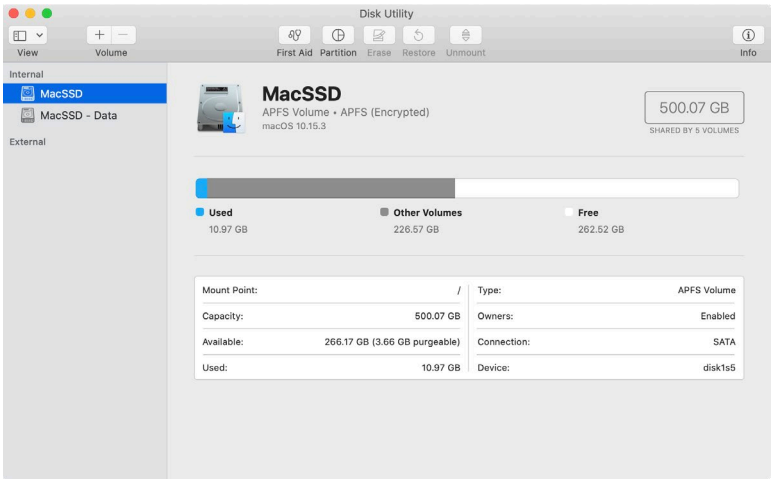


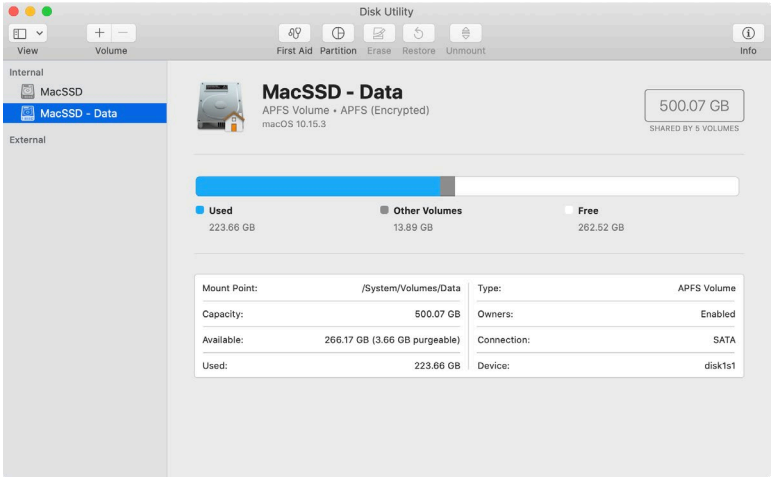
Hard drives and storage devices are shown in the list on the left side of the Image view. Device volumes or partitions are shown below their associated hard drive or storage device.

For more information, see Creating an Image.

Views of System Volume and Data Volume on Mac Computers

As of macOS Catalina 10.15, the operating system runs in a read-only system volume, separate from other files. This increases protection for the operating system. When a computer is upgraded to macOS Catalina or later, a second volume is created and some files may move to a Relocated Items folder. The boot volume is effectively split into two pieces. On the Desktop it appears as one volume, but looking at it with Disk Utility, it is readily apparent there are two volumes.





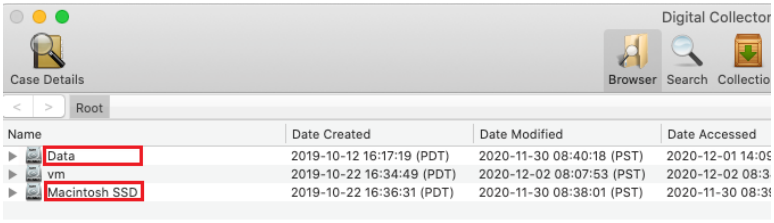
The volume name that appears on the Desktop appears in both volumes seen in Disk Utility. In Disk Utility, the second volume has "- *Data*" appended to the volume name, for example *MacSSD - Data* or *Macintosh SSD - Data*. For more information, see https://support.apple.com/en-us/HT210650.

If FileVault 2 is enabled, the same credentials unlock both volumes in Digital Collector.

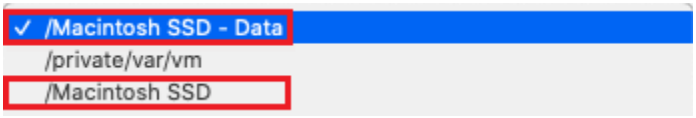
Both of the volumes appear in all the views in Digital Collector. The system volume appears with the volume name. The name of the data volume differs slightly among the views in Digital Collector.

Note: While there may be some data overlap between the volumes, you should examine both volumes to ensure that no important files are overlooked.

In the Browser view, the name of the data volume is *Data*.

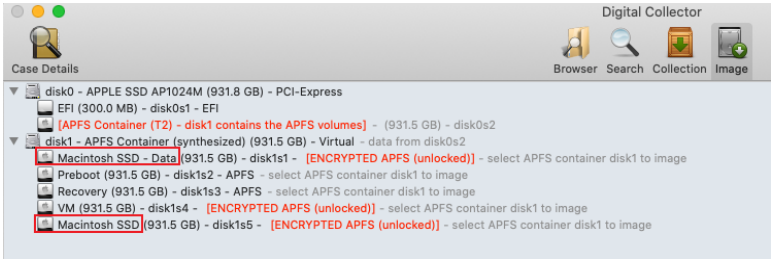


In the Search view, the name of the data volume is the same as in Disk Utility, */<VolumeName> - Data*. The data volume is selected by default in the Location list. Be sure to search both volumes to ensure that no important files are overlooked.



In the Collection view, the name of the data volume is *Data*. Both volumes appear in the System Files list under MACOS VOLUMES.

In the Image view, the name of the data volume is the same as in Disk Utility, */<VolumeName> - Data*. Both volumes appear as two separate slices.



Tools View

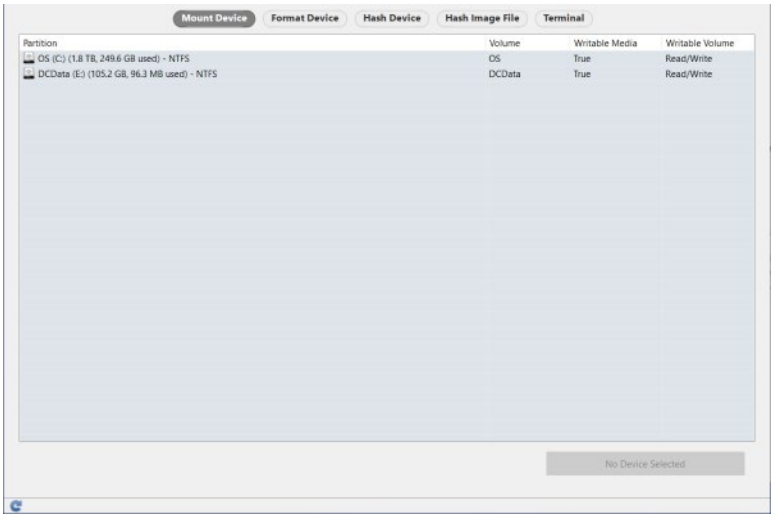
The Tools view in Cellebrite Digital Collector provides a variety of advanced acquisition tools developed for experienced forensic examiners.

- Mount Device
- Format Device
- Hash Device
- Hash Image File
- Terminal

Warning: These tools are meant for the advanced forensic examiner. Improper tool use may result in evidentiary data loss or corruption.

Some of these tools are useful only when you start (boot) the source computer from the Digital Collector device, as they are unusable or inappropriate for use during a live acquisition.

In the toolbar, click **Tools**. The Tools view appears, showing a tab for each advanced tool.



For more information, see Tools.

Refresh the Device List

You can refresh the list of devices shown in Cellebrite Digital Collector any time you like for any view but Case Details.

In the bottom left corner of the Digital Collector window, click , (**Refresh Device List**).

Setting Preferences on a Mac Computer

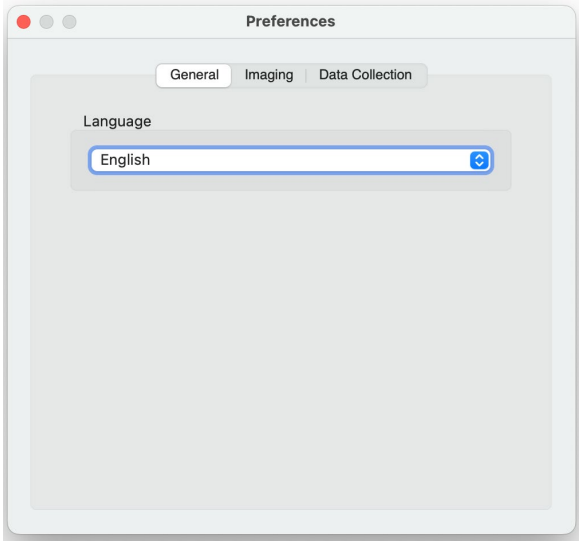
Cellebrite Digital Collector preferences are stored on the Digital Collector SSD in a database file named *com.cellebrite.DigitalCollector.settings*, which is in the *WINDOWS APP* partition. You may set preferences on either a Mac or a Windows computer; setting preferences on one platform sets them for the other.

In the menu bar, click **Digital Collector > Preferences**. These are the tabs on the Preferences window.

- General
- Imaging
- Data Collection

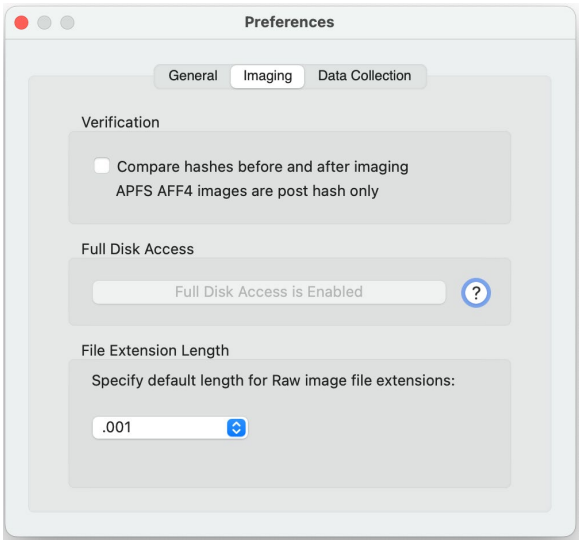
Set Language Preference

On the General tab in the Preferences window, choose the appropriate language in the **Language** field.



Set Imaging Verification Preference

To automatically validate data before and after imaging, click **Imaging** on the Preferences window, and then mark the **Compare hashes before and after imaging** checkbox. By default, hashing happens inline with imaging and there is no need for before-and-after hashing. Later versions of the Mac operating systems require full disk access.

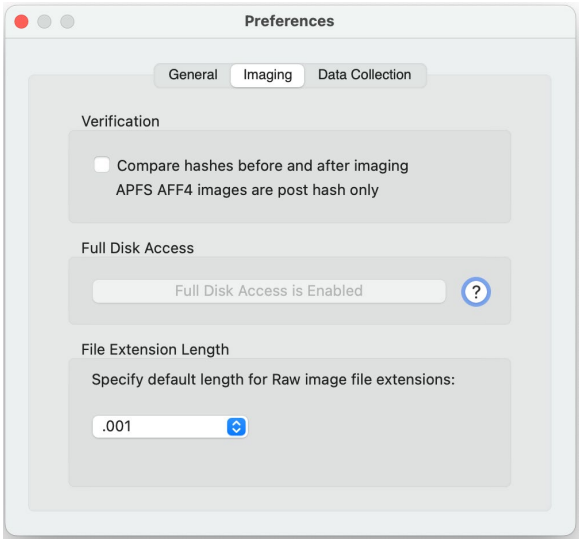


Note: The AFF4 image format is for imaging Mac computers with APFS Fusion or with T2 chips. Pre-image hashing is not valid for APFS Fusion drives because they are synthesized containers. Pre-imaging hashing on computers with T2 chips would result in a hash of encrypted data that could never be decrypted and is therefore also not valid. Digital Collector will hash the data collected in the AFF4 image file.

This is an example of a post-acquisition Activity window with the verification preference enabled.

Set Length for Raw Image File Extensions

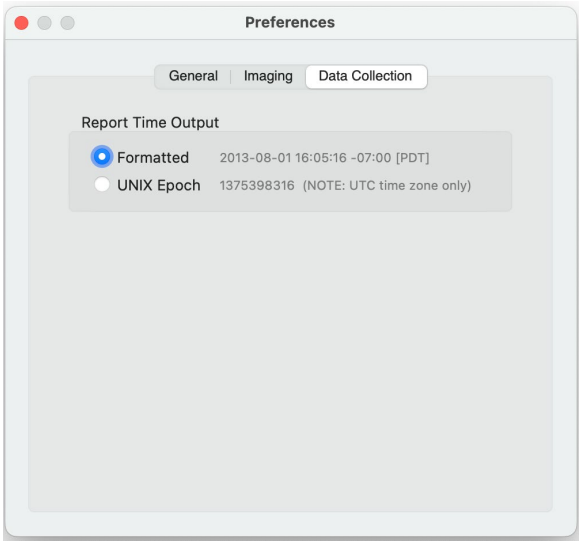
To specify the default length of file extensions for raw image files, click **Imaging** on the Preferences window, and then choose the appropriate option in the **Specify default length for Raw image file extensions** field.



Set Report Time Output Preference

You can choose how timestamps are represented in report output from Digital Collector. Formatted is the default.

To change it to UNIX Epoch timestamps (UTC only), click **Data Collection** on the Preferences window, and then select **UNIX Epoch**.



Setting Preferences on a Windows Computer

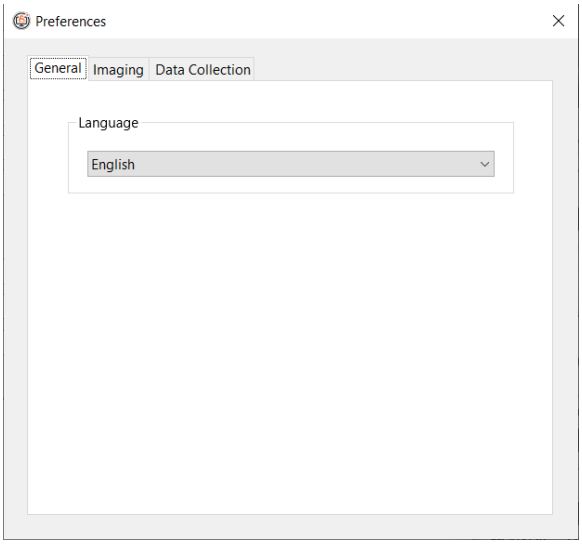
Cellebrite Digital Collector preferences are stored on the Digital Collector SSD in a database file named *com.cellebrite.DigitalCollector.settings*, which you can find in the *WINDOWS APP* partition. When you set preferences, they apply to Digital Collector for both Mac and Windows computers. Setting preferences in Digital Collector on one platform effectively sets them for the other as well.

In the menu bar, click **Edit > Preferences**. These tabs are on the Preferences window.

- General
- Imaging
- Data Collection

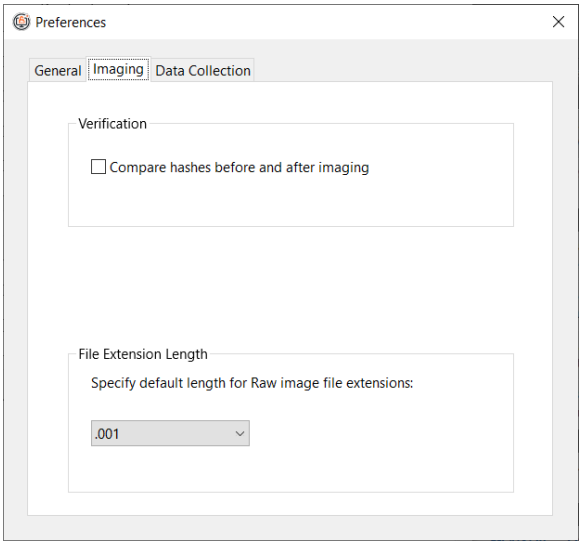
Set Language Preference

On the General tab in the Preferences window, choose the appropriate language in the **Language** field.



Set Imaging Verification Preference

To automatically validate data before and after imaging, click **Imaging** on the Preferences window, and then mark the **Compare hashes before and after imaging** checkbox.



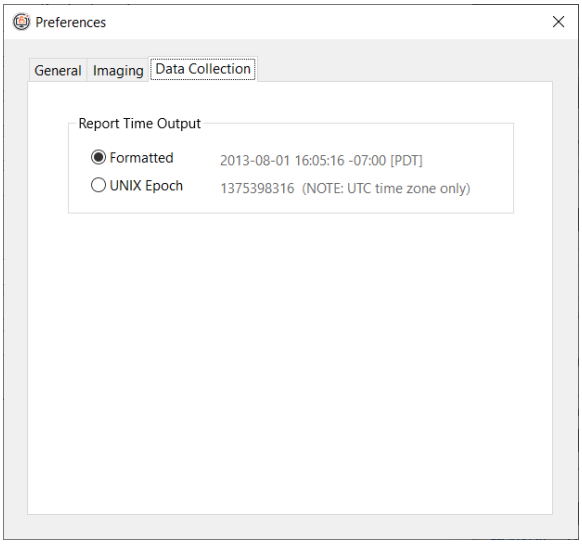
Set Length for Raw Image File Extensions

To specify the default length of file extensions for raw image files, click **Imaging** on the Preferences window, and then choose the appropriate option in the **Specify default length for Raw image file extensions** field.

Set Report Time Output Preference

You can choose how timestamps are represented in report output from Digital Collector. Formatted is the default.

To change it to UNIX Epoch timestamps (UTC only), click **Data Collection** on the Preferences window, and then select **UNIX Epoch**.



Launching Digital Collector on a Live Computer

You may need to capture volatile user-specific data, system artifacts, and Random Access Memory (RAM) contents while a source computer is running. With Cellebrite Digital Collector, data collected during a live acquisition may be saved to a forensic image.

Digital Collector can acquire RAM from macOS computers up to version 10.15.7.

When time is limited, you may select and acquire specific data from a live source computer using only the Digital Collector solid state drive (SSD) and a destination collection device, or even the *DCData* partition on the Digital Collector SSD itself if the capacity of that partition is adequate.

Obtain an administrator username and password for the source computer when possible. Launching Cellebrite Digital Collector from an administrator account allows the software to run with root privileges.

You can acquire data directly from a live source computer or start (boot) your host computer with Cellebrite Digital Collector to acquire data from a connected source computer by connecting the Digital Collector SSD to the computer. The partitions on the Digital Collector SSD appear in the file system. Before you begin, you should understand the partitions on the Digital Collector SSD. For more information, see Digital Collector Device.

Connect a storage device to serve as the collection's destination, then launch the Digital Collector application.

During a live acquisition, the source computer must remain connected to your host computer throughout the entire process.

Note: Because Digital Collector can capture data selected from any computer the Digital Collector SSD is attached to, proceed carefully to prevent inadvertently capturing data from the host computer itself.

Note: Running Digital Collector on a live computer makes changes to artifacts on that computer. Therefore, it is important to thoroughly understand and document connections to the Digital Collector SSD. For more information, see Appendix: Changes to Live Computers.

This chapter provides these topics.

Launch Digital Collector on a Live Mac Computer

You may connect the Digital Collector device to a running source Mac computer, or to your own running host computer.

After Digital Collector is launched on a source computer, you can obtain a logical data collection.

You can also create images of live APFS volumes that are mounted read/write. During this process the volume is locked/frozen. This can cause behavior that seems unusual until imaging is complete.

Note: Before you begin, you must ensure that the disk being imaged will not try to shut down, has an uninterrupted supply of power, and that the screen never goes to sleep. If you don't take these precautions, you may not see the notification that the image is complete or the image may fail to complete.

Note: To create an image while Digital Collector is running live on macOS 12 Monterey, you must first disable System Integrity Protection (SIP). You can search online for instructions.

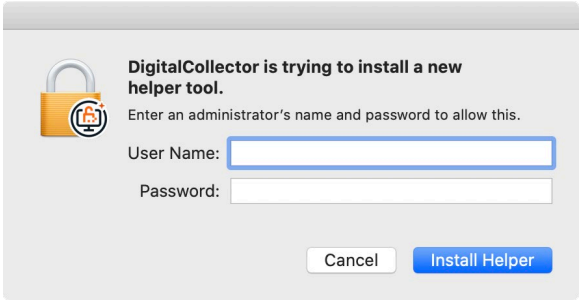
Launch Cellebrite Digital Collector from an administrator account when possible, so the software runs with administrator-level permissions. After you successfully enter an administrator password, Digital Collector runs with root privileges.

Before you begin: You should be aware of capabilities and limitations for launching Digital Collector from a live source computer. These are determined by the macOS that is running on the source computer. For more information, see Imaging Considerations for macOS.

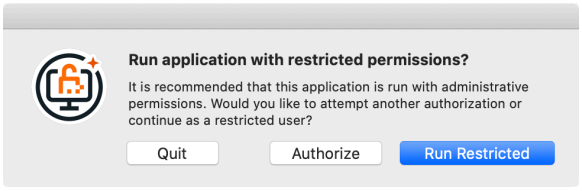
Warning: Running Digital Connector directly connected to a live, source computer results in changes. For more information, see Appendix: Changes to Live Computers.

If the End User License Agreement has not been accepted yet for Cellebrite Digital Collector, you can do so when it launches. For more information, see Accepting the Digital Collector End User License Agreement.

1. Connect the Digital Collector SSD to a USB port on the computer.
2. Use Finder to browse to the *MacOS App* partition on the SSD, and then double-click **DigitalCollector.app**.
   A dialog box appears for you to provide login credentials for an administrative user account on the computer.

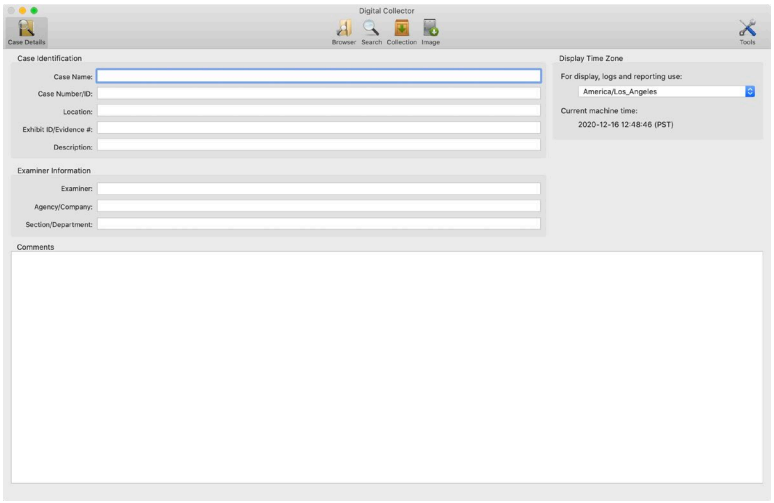


3. Choose the appropriate action.
   - If you have administrator credentials, type them in the **User Name** and **Password** fields, and then click **Install Helper**.
   - If you don't have administrator credentials, click **Cancel**.
     A restricted permissions confirmation dialog box appears.



   - To run Cellebrite Digital Collector with restricted permissions (permissions for the user who is currently logged in), click **Run Restricted**.

4. If the End User License has not been accepted yet, you can do so now.
   The Case Details view appears in the Digital Collector window.



You can provide information on the Case Details view and then collect data from the live source computer. For more information, see Case Details View.

- If Digital Collector is directly connected to the live source computer, you can obtain a logical data collection or create an image. For more information, see Collecting Data from a Source Computer and Imaging Mac Computers.
- If the live source computer is connected in target disk mode (TDM) to a host computer running Digital Collector, you can obtain a logical data collection or you can create an image. For more information, see Imaging Mac Computers.

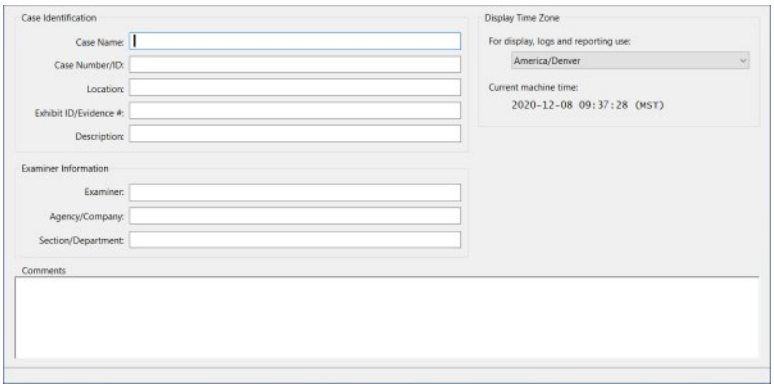
Launch Digital Collector on a Live Windows Computer

On a live Windows computer, you must launch Cellebrite Digital Collector from an administrator account. It will not run with a user account. Digital Collector runs with administrator privileges.

If you do not have an administrator password for the computer, you can start the computer from the Digital Collector solid state drive (SSD). For more information, see Starting a Computer with Digital Collector.

If the End User License Agreement has not been accepted yet, you can do so when Cellebrite Digital Collector launches. For more information, see Accepting the Digital Collector End User License Agreement.

1. Connect the Digital Collector SSD to a USB port on the computer.
   Ignore any prompts to scan or format the SSD or to set AutoPlay defaults.
2. Use File Explorer see the *WINDOWS APP* partition.
3. In the *WINDOWS APP* partition, double-click **DigitalCollector.exe**.
4. Choose the appropriate action.
   - If User Account Control (UAC) is not enabled, go to Step 5.
   - If User Account Control (UAC) is enabled and the logged-in user
     - has administrative permissions, click **Yes**. Digital Collector launches.
     - does not have administrative permissions, enter an administrator password, clicking **More Choices** if necessary to see all the user accounts for this computer. Digital Collector launches.
5. If the Digital Collector EULA window appears, you can either click **Agree** or mark the checkbox for **Permanently Accept** and then click **Agree**.
6. The Case Details view appears in the Digital Collector window.



For more information, see Case Details View.

Starting a Computer with Digital Collector

You may connect a source computer to your own host or analysis computer and treat the source computer like an external drive to create an image of it or to create a logical data collection. To do this, you must start (boot) your host computer from the Cellebrite Digital Collector solid state drive (SSD) before you connect it to the source computer. If the source computer is a Mac, you must also place it in target disk mode (TDM) before you connect it to your host computer. To write-protect the source computer, you should use either a hardware write-blocker or a software-based write-blocking solution.

Note: TDM does not exist on M1 Mac computers.

If you do not have a host or analysis computer, you may boot a source computer from the Digital Collector SSD and save the image or logical collection to an external device using only the source computer itself. Because Digital Collector boots into a forensically sound environment, no additional write-blocking software or hardware is necessary. You only need the source computer, the Digital Collector SSD, and a destination device to perform a static data acquisition. The Digital Collector SSD itself has a partition, *DCData*, that can be the destination if it has enough available space to hold the image or the logical collection. For more information, see Digital Collector Device.

Before you begin, you should review the Other Equipment topic.

This chapter provides these topics.

- Start a Mac Computer with Digital Collector
- Connect a Source Mac Computer in Target Disk Mode
- Start a Windows Computer with Digital Collector

Start a Mac Computer with Digital Collector

These are the reasons to start a Mac computer with the Cellebrite Digital Collector solid state drive (SSD):

- To start your own host computer with Digital Collector before you connect it to a source computer as an external hard drive to image or collect data from. Before you begin, you must put the source computer into target disk mode (TDM). For more information, see Connect a Source Mac Computer in Target Disk Mode.

  Note: M1 Mac computers do not have TDM.

- If you don't have a host computer, or if you don't have the administrator password for the source computer, you can start (boot) a source computer directly from the Digital Collector SSD.

If the Mac computer is a late 2017 to 2020 model, it may have a T2 security chip. One of the functions of the T2 chip is to prevent the computer from booting to external devices, including Digital Collector. You can remove this restriction in the Startup Security Utility, in the computer's *Recovery* partition. You need an admin password to access the Startup Security Utility. To start the *Recovery* partition, press CMD+R while starting the computer. Then change the settings to **No Security** and **Allow booting from external media**. For more information, see https://support.apple.com/en-us/HT208198.

The most forensically sound method for acquiring data from the source computer is to place it in target disk mode and not change the security settings. If you do change the secure boot settings and later want to change it back from No Security to Full Security, Apple requires an internet connection.

Before you begin: If a source computer has only one USB port, you may use a powered USB hub. When you work with Mac computers, genuine Apple cables and adapters are required. For more information, see Other Equipment.

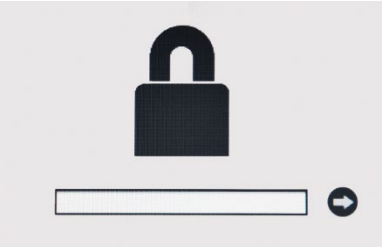
Warning: Do not use a wireless keyboard. Keystrokes on wireless keyboards may not be transmitted quickly enough to halt the boot process and prevent the computer from starting from its own operating system.

Warning: Review this entire procedure. If a source computer shows signs of starting from its operating system and not with Digital Collector, you must be ready to shut it down immediately.

Warning: Newer Mac laptops start immediately upon opening the lid. This includes Intel, T2, and M1 Macs.

1. Ensure the computer is not running and is connected to a power source.
2. Connect the Digital Collector SSD to a USB port on the host computer or directly to the source computer if there is no host.
3. Connect an external storage device, if needed, to the host computer or directly to the source computer if there is no host. This is the destination where the image or logical data collection will be stored.
4. On the computer connected to the Digital Collector SSD, take either of these actions:
   - Press the power button and immediately hold down the OPTION key.
   - On an M1 computer, press and hold the power button.

5. Release the OPTION key or the power button when either of these appears.
   - A window appears where you can type the firmware password, if it is enabled.



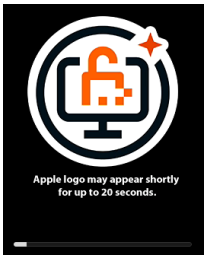
     Type the firmware password. If you do not have the password for the source computer, you cannot proceed.

   - The Startup Manager appears.

6. Choose the appropriate action.
   - If the computer is an M1 Mac, select the **DC ARM Boot** volume and then click **Continue**.
   - If the computer is not an M1 Mac, select the **Cellebrite Digital Collector 3.4** volume and then click the arrow below it.

Warning: Do not select the EFI volume, which runs properly only on Windows computers.

7. Take the appropriate action based on the response to Step 6.

Response	Action
The logo for Cellebrite Digital Collector appears along with a progress bar. 	The computer has started successfully from Digital Collector. The Case Details window appears. You can now create an image or obtain a logical data collection. For more information, see these topics: • Imaging Mac Computers • Collecting Data from a Source Computer
The Apple logo appears before the Digital Collector logo.	If the computer is an older Mac, it is booting to its own operating system and not to Digital Collector. Press and hold the computer's power button immediately to stop the computer. (On newer Mac computers, the Apple logo appears during the boot process even when it is starting from the Digital Collector SSD.)
A gray or black screen with a slashed circle appears.	The computer has failed to boot to the Digital Collector boot volume. Choose one of these actions: • If the source computer is an Intel Mac, try this process again with the Legacy partitions. You can also place the Intel Mac in Target Disk Mode and connect it to a host computer that was booted from Digital Collector. For more information, see Connect a Source Mac Computer in Target Disk Mode. Do not select the EFI volume. • If the source computer is an M1 Mac, the model may not be supported yet.

Connect a Source Mac Computer in Target Disk Mode

To obtain a decrypted physical image or a decrypted logical data collection, you can put the source computer in target disk mode (TDM) and connect it to your host computer running Cellebrite Digital Collector. This is possible even for Mac computers with a T2 chip.

Note: M1 Mac computers do not have TDM.

To write-protect the source computer, you should start (boot) the host computer with Digital Collector. For more information, see Start a Mac Computer with Digital Collector.

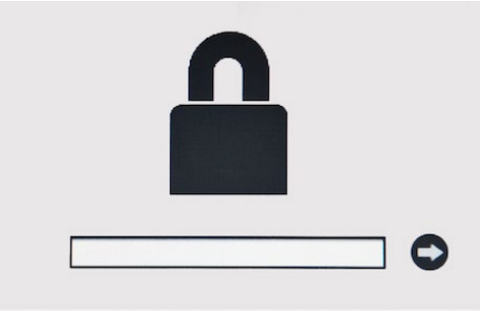
If you must run Digital Collector on a live host computer, use either a hardware write-blocker or a software-based write-blocking solution. For more information, see Other Equipment.

For related information about Mac computers, see these topics from Apple.

- https://support.apple.com/en-us/HT204455
- https://support.apple.com/guide/mac-help/transfer-files-mac-computers-target-disk-mode-mchlp1443/mac

Before you begin, ensure the source computer is not running and is connected to a power source. Also ensure that Digital Collector is running on the host computer.

1. On the source computer, press the power button and immediately press and hold OPTION.
2. If this window appears, a firmware password is required.



   Release the OPTION key and type the firmware password. If you do not have the password, you cannot proceed.

3. Release the OPTION key and press T.
4. With a genuine Apple Thunderbolt cable, connect the source computer to the host computer.

Note: If the host computer has a USB-C port, the most reliable cable is the Apple USB-C TB3 cable. If the host computer has a Thunderbolt 2 port, the most reliable connection is the Apple TB cable and Apple TB3 to TB2 adapter.

When Digital Collector detects the connect source computer in TDM, you can either obtain a decrypted physical image or a decrypted logical collection.

Important: If the source computer has Apple File System (APFS), you must select the synthesized APFS container to image to ensure that the data is decrypted.

For more information, see these topics.

- Imaging Mac Computers
- Collecting Data from a Source Computer

Start a Windows Computer with Digital Collector

You can start your own host computer with the Cellebrite Digital Collector solid state drive (SSD) before you connect it to a source computer, to treat it as an external hard drive that you can image or collect data from.

You can also start (boot) a source computer directly from the Digital Collector SSD if you don't have the administrator password.

Note: When Digital Collector is used to start a Windows computer, it cannot detect eMMC drives, such as those used in Lenovo Ideapad style devices. It also cannot display Intel Rapid Storage Technology (RST) RAIDs. You can create images in both these scenarios by starting Digital Collector on such computers when they are running live. Digital Collector can acquire images of Windows computers encrypted with BitLocker; however, it cannot decrypt those images. You can decrypt those images with Cellebrite Inspector.

Before you begin:

- Review this entire procedure. If a source computer shows signs of booting to its operating system and not to Digital Collector, you must be ready to shut it down immediately.
- You need to know how to start the source or the host computer so that the boot menu appears. This is necessary so that you can select Digital Collector to boot from, rather than the computer's own operating system. You can do this by repeatedly pressing the correct key or keys during startup. The exact boot key varies among manufacturers and computer models, but these keys are often used: ESC, F2, F10, and F12. If none of these commonly used boot keys reveal the boot menu, you can search online for the manufacturer and model of the source or the host computer.
- You should also review the Other Equipment topic.

Warning: Do not use a wireless keyboard. Keystrokes on wireless keyboards may not be transmitted quickly enough to halt the boot process and prevent the computer from booting to its internal operating system.

Among Windows computers, there are a wide variety of start configurations, as well as the sequence and appearance of BIOS screens and Boot Menus. Therefore, this topic provides general guidance.

1. Ensure the source or host computer is not running and is connected to a power source.
2. Connect the Digital Collector SSD to a USB port on the host computer or directly to the source computer if there is no host.
3. Connect an external storage device, if needed, to the host computer or directly to the source computer if there is no host. This is the destination where the image or logical data collection will be saved.
4. On the computer connected to the Digital Collector SSD, press the power button and immediately begin repeatedly pressing the boot key until you see the BIOS screen or Boot Menu. If you see the BIOS screen, you can find the Boot Menu there.
5. In the Boot Menu, select **Cellebrite Digital Collector 3.4**.
6. The computer boots from Digital Collector.
   It may take a few moments before Digital Collector appears.

Proceed with triage, collecting data, or creating an image.

Collecting Data from a Source Computer

Forensically significant user data and system artifacts are located in many different places in computer file systems. Manually locating and selecting such data during a forensic acquisition may be both daunting and time-consuming, especially when you are collecting data from a live computer under time constraints. For more information, see Launching Digital Collector on a Live Computer.

Cellebrite Digital Collector makes this task quick and simple. This is especially important when collection time is limited. The Collection view automatically targets these data categories.

- User Files
- System Data
- System Files
- Additional Files

You can add files and folders to the Additional Files category from the Browser and Search views as well as from the Collection view. You can also create and use custom file filters and collection templates, which make it easier and faster to select items to collect. For more information, see Custom File Filters and Collection Templates.

For more information, see these topics.

- Collection View
- Browser View
- Search View

Note: Obtaining a decrypted logical collection is the same for all Mac computers, even those with a T2 chip. If FileVault 2 is enabled, you must unlock the encrypted volume to decrypt the data before you can create a logical collection. For more information, see Mount Device Tool.

This chapter provides these topics.

- Selecting User Files
- Selecting System Data
- Selecting System Files
- Selecting Additional Files and Folders
- Collecting Selected Data
- Verifying Collected Data

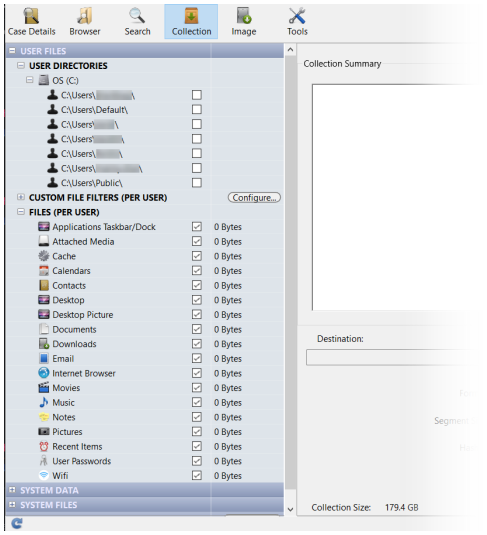
Selecting User Files

On every computer, each user has their own files and folders. Cellebrite Digital Collector allows a forensic examiner to identify all user accounts and then target and collect data corresponding to specific users.

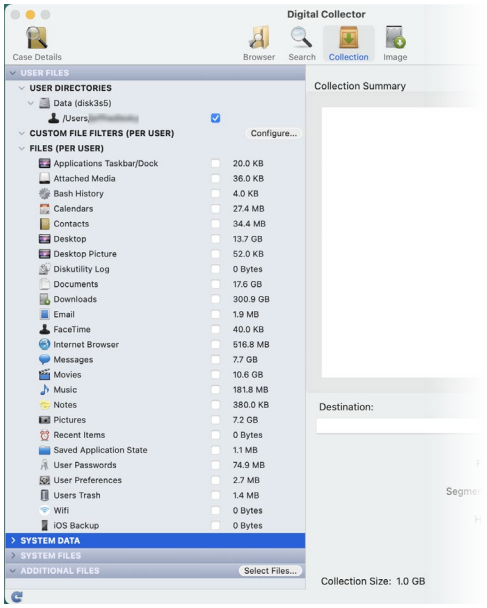
Tip: You can select or deselect everything in the entire list in the Collections view by using the context menu (right-click anywhere in the list) and choosing the appropriate action.

In the toolbar, click **Collection** and then expand the **USER FILES** section of the list on the left side of the Collection view.

The USER FILES section of the list looks like this on Windows computers.



The USER FILES section of the list looks like this on Mac computers.



These are the sections within the USER FILES list.

- USER DIRECTORIES, where user accounts are grouped according to which internal drive or attached device contains each user directory. Expand or collapse the list for any drive or device to show or hide the associated user accounts.
- CUSTOM FILE FILTERS (PER USER) where you can select custom file filters, which make it easier and faster to select items to collect. For more information, see Custom File Filters and Collection Templates.
- FILES (PER USER), where categories of file types are listed.

These sections of the list work together.

1. In the USER DIRECTORIES section, mark the checkbox to the right of the path name to select specific user accounts to collect data from.
2. Choose either or both of these actions:
    - In the FILES (PER USER) section, mark the checkbox to the right of each item to collect for the selected users.
    - In the CUSTOM FILE FILTERS (PER USER) section, mark the checkbox to the right of a custom file filter.

For example, you could select two of the user directories and then select only Documents, Downloads, and Pictures. Or you could select two of the user directories and then select one custom file filter. The collection is limited to only the targeted items for the selected users.

You can apply a collection template as an alternative or addition to custom file filters. For more information, see Custom File Filters and Collection Templates.

Look in the **Collection Size** field at the bottom of the Collection view, to the right of the list. If you deselect a user or select another user, or if you deselect or an item or select another item, the size of the collection is recalculated to reflect excluding or including the selected files for the selected users. When time is limited, you can quickly triage user data according to importance. The larger the size, the longer it will take to collect.

Options for Collecting User Files

These are the preset options for user files that can be collected.

Option	Description	Mac	Windows
Applications Taskbar/Dock	Collect the user account's Dock or Taskbar application preference settings	✓	✓
Attached Media	Collect attached device history	✓	✓
Bash History	Collect command line history (bash shell)	✓	
Cache	Collect temporary files		✓

Option	Description	Mac	Windows
Calendars	Collect iCal calendar events and attachments from macOS Collect *AppData\Local\Packages\microsoft.windowscommunicationsapp_8wekyb3d8bbwe* from MSOutlook on Windows Collect *AppData\Local\Comms\Unistore* from the Windows 10 Mail app	✓	✓
Contacts	Collect Contact data	✓	✓
Desktop	Collect all files located on the user account's Desktop	✓	✓
Desktop Picture	Collect the user account's Desktop wallpaper	✓	✓
Diskutility Log	Collect all user actions executed from the Disk Utility application	✓	
Documents	Collect all files/folders in the user account's *Documents* folder Collect all TextEdit* application files	✓ ✓	✓
Downloads	Collect all files/folders in the user account's *Downloads* folder	✓	✓
Email	Collect Microsoft Outlook email and cache data Collect Microsoft Entourage email, downloads, and cache data Collect Mac Mail application email and downloads	✓ ✓ ✓	✓
FaceTime	Collect FaceTime*	✓	
Internet Browser	Collect Google Chrome internet history, cookies, and cache Collect Microsoft Edge internet history, cookies, and cache Collect Internet Explorer internet history, cookies, and cache Collect Firefox internet history, cookies, and cache Collect Safari internet history, bookmarks, cookies, cache, and more.	✓ ✓ ✓	✓ ✓ ✓ ✓
Messages	For iMessage and iChat, collect logs, files, .plist file, and cache files	✓	

Option	Description	Mac	Windows
Movies	Collect all files in the user account's *Movies* folder Collect QuickTime application files	✓	✓
Music	Collect all files in the user account's *Music* folder	✓	✓
Notes	Collect user account's Notes* Collect user account's Stickies (sticky note) application data	✓ ✓	 ✓
Pictures	Collect all files in the user account's *Pictures* folder Collect all user account Photo Booth application picture files Collect all user account Preview* application picture files	✓ ✓ ✓	✓
Recent Items	Collect data in the user account's Recent Items menu	✓	✓
Saved Application State*	Collect application window settings and data from the last time applications were used	✓	
User Passwords	Collect user account password files	✓	✓
User Preferences	Collect all user-defined application preferences	✓	
Users Trash	Collect all items in the user account's *Trash* folder	✓	
Wifi	Collect Wifi data	✓	✓
iOS Backup	Collect all user iOS backup folders	✓	

* Denotes data collected from the *~/Library/Containers/* directory, if it exists on a Mac computer.

Custom File Filters and Collection Templates

Custom file filters and collection templates can make it easier and faster to select items to collect. Once you establish these, you can rely on them to more quickly and consistently select items to collect. This can also mean that more junior examiners can work more independently to consistently select appropriate items. Additionally, the resulting data collection may be smaller while still focusing on relevant data.

Both custom file filters and collection templates are saved in the settings file on the Digital Collector device (dongle). This ensures that they are always available as you collect data from different computers, regardless of whether they run Mac or Windows.

In the Collection view, the SYSTEM DATA and USER FILES groups have exchanged locations in the list of items to collect. USER FILES is now at the top of the list. This makes it easier to use custom file filters in conjunction with selecting the appropriate user.

The new CUSTOM FILE FILTERS (PER USER) section appears in the USER FILES group.

Custom file filters and collection templates work on both booted and live Mac and Windows computers. The same filters and templates can be used on either platform. Any aspects that do not apply to the source computer due to platform differences are simply ignored. For example, when a template is defined to collect the Windows registry, that yields no result on a basic Mac computer. However, if a Mac computer has a Bootcamp volume that Digital Collector recognizes, the same template can collect the Windows registry from that volume.

For custom file filters or templates to select files, you must also select at least one user in the USER DIRECTORIES section of the list of items to collect. Only files for the selected user will be collected.

Filters look for files based on these user locations.

- Desktop
- Documents
- Downloads
- Library
- Videos
- Music
- Pictures
- Home

Templates look for files based on groups or items you select as well as any custom file filters you select. When you apply a template, you must also select at least one user in the USER DIRECTORIES section of the list of items to collect.

You can apply only one template at a time.

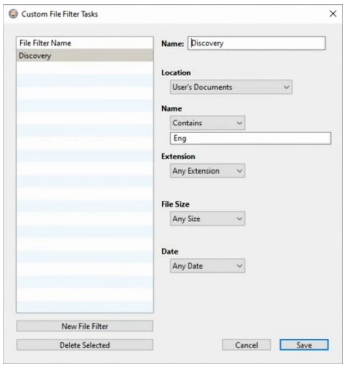
For more information, see these topics:

- Create and Manage Custom File Filters
- Collection Templates

Create and Manage Custom File Filters

Before you begin, you should understand the information in this topic: Custom File Filters and Collection Templates.

1. Take one of these actions.
   - In the Menu bar, click **Templates > Configure Custom File Filters**.
   - To the right of CUSTOM FILE FILTERS (PER USER) in the list of items to collect, click **Configure**.
   - Open the context menu from CUSTOM FILE FILTERS (PER USER) and then click **Configure Custom File Filters**.
   - The Custom File Filter Tasks dialog box appears.



2. Take any of these actions.

Action	Steps
Create a file filter	These fields are similar to the fields on the Search view. a. Click **New File Filter** and then type a name for the file filter in the **Name** field. b. In the **Location** field, select the location that items will be collected from. c. In the **Name** field, set the criteria for the file name. d. In the **Extension** field, set the criteria for the file extension. e. In the **File Size** field, set the criteria for the file size. f. In the **Date** field, set the criteria for the date. These new options may be most useful. These options are also available in the Search view. • last day • last week • last month • last year g. Click **Save**. Note: When you boot a Windows computer with Digital Collector, filtering on Date Created is not supported.

Action	Steps
Change a file filter	a. In the **File Filter Name** list, elect a file filter and change any data, including the name. b. Click **Save**.
Delete a file filter	Select a file filter and click **Delete Selected**.

After you have created custom file filters, you can select them the way you would any items in the list. Selecting a custom file filter automatically selects the items defined for that filter.

You can see detailed information about what will be collected in the Collection Summary box.

The size of the collected set of items appears to the right of the checkbox for the custom file filter. As with all other items in the list, if you select or deselect any users, the size is recalculated accordingly.

Collection Templates

Before you use collection templates, you should understand custom file filters as well. For more information, see Custom File Filters and Collection Templates.

There are two approaches to defining collection templates. You may prefer to define collection templates that pertain to either the Mac or the Windows platform or you can define single collection templates that apply to both platforms at the same time. The latter approach is possible because the list of items is not restricted by the platform of the computer you happen to be using while you define collection templates. This means that you can define a single template with all the appropriate items selected for both the Mac and Windows platforms. When you apply the collection template to a source computer, the template items that pertain to the computer's platform are selected. The benefit is that one person with expertise can set up collection templates on Digital Collector devices used by more junior examiners.

You can create a collection template based on any selections you have currently made in the Collection view or you can use the Collection Templates dialog box.

For more information, see these topics:

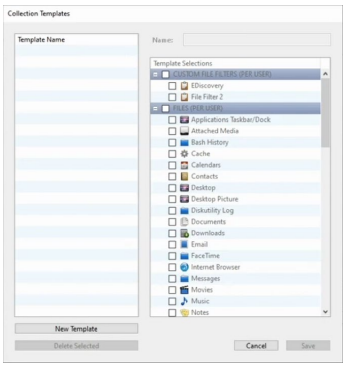
- Save Current Selections as a Template
- Create and Manage Collection Templates
- Apply a Collection Template

Save Current Selections as a Template

If you have made selections on the Collection view that you think you'll likely use often in the future, there are two ways you can save them as a collection template.

- In the Menu bar, click **Template > Save Current Selections as Template**.
- Open the context menu from the list of items to collect and then click **Save Current Selections as Template**.

  The Collection Templates dialog box appears.



1. In the **Name** field, type a descriptive name for this template.
2. Review the items the **Template Selections** list and if necessary, mark or unmark the checkboxes for any items, and then click **Save**.

Create and Manage Collection Templates

You can create, change, and delete collection templates. Collection templates can include any custom file filters you have created.

1. Take one of these actions.
   - In the Menu bar, click **Templates > Configure Collection Templates**.
   - Open the context menu from the list of items to collect and then click **Configure Collection Templates**.
2. In the Collection Templates dialog box, you can take any of these actions.

Action	Steps
Create a collection template	a. Click **New Template**. b. In the **Name** field, type a descriptive name for this collection template. c. In the **Template Selections** list, mark the checkbox for any items, groups, or custom file filters to include in this template and then click Save.
Change a collection template	a. In the **Template Name** list, select the appropriate template. b. As appropriate, change the name or mark or unmark the checkboxes to change what is included in this template c. Click **Save**.

Action	Steps
Delete a collection template	In the **Template Name** list, select the appropriate template and then click **Delete Selected**.

Apply a Collection Template

After you have defined a collection template, you can apply it to quickly and easily select the associated items to be collected from the source computer.

1. Take one of these actions.
   - In the Menu bar, click **Templates > Apply Collection Template**.
   - Open the context menu from the list of items to collect and then click **Apply Collection Template**.
2. Select the appropriate collection template. You can apply only one template at a time.

If necessary, you can mark or unmark the checkboxes for any items, groups, or custom file filters.

You can see detailed information about what will be collected in the Collection Summary box.

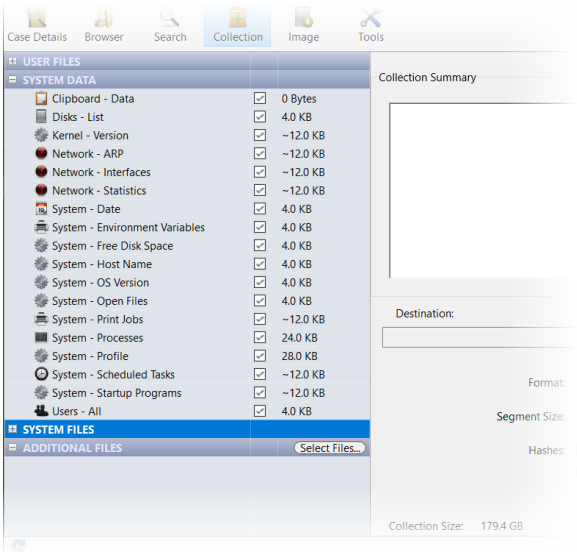
If you select or deselect any users, the collection size is recalculated accordingly.

Selecting System Data

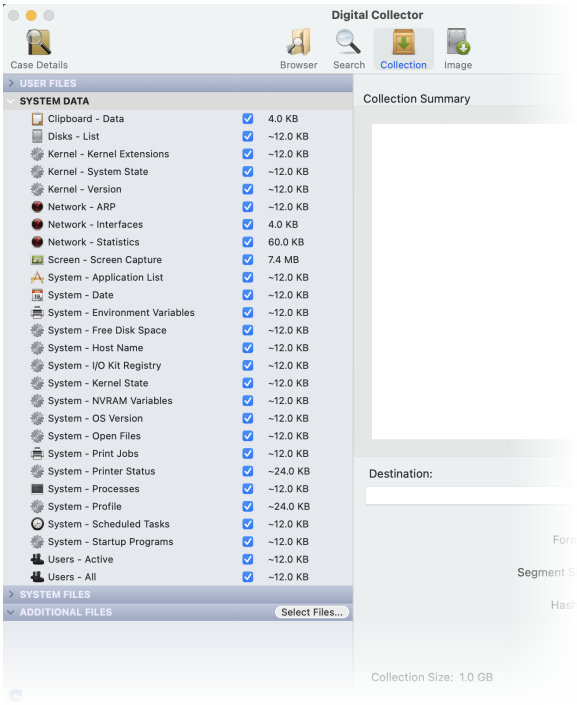
Cellebrite Digital Collector has defined many preset groups of system data that you can select for collection.

In the toolbar, click **Collection**, and then expand the **SYSTEM DATA** section of the list on the left side of the Collection view.

The SYSTEM DATA section of the list looks like this on Windows computers.



The SYSTEM DATA section of the list looks like this on Mac computers.



You can select a system data collection option in the list to see details or a preview in the Collection Summary section, on the right side of the Collection view.

To select system data, mark the checkbox to the right of each option to be collected.

You can select or deselect all options in all sections of the list in the Collections view by using the context menu (right-click anywhere in the list) and choosing the appropriate action.

When time is limited, you can quickly triage system data according to importance. Look at the total size shown for each option and look at the Collection Size field at the bottom of the Collection view, to the right of the list. When you mark or unmark the checkbox to the right of an option, thereby including or excluding it, Digital Collector automatically recalculates the size of the entire collection. The larger the size, the longer it will take to collect.

Options for Collecting System Data

These are the preset options for collecting system data.

Option	Description	Mac	Windows
Clipboard - Data	Collect current clipboard data	✓	✓
Disks - List	Collect a list of all attached drives and storage devices	✓	✓
Kernel - Kernel Extensions	Collect a list of installed kernel extensions (kext files)	✓	
Kernel - System State	Collect current kernel state (state specs, min/max capabilities)	✓	
Kernel - Version	Collect current kernel information	✓	✓
Network - ARP	Collect current Address Resolution Protocol (IP to MAC address table) for the primary interface	✓	✓
Network - Interfaces	Collect a list of system network interfaces	✓	✓
Network - Statistics	Collect active Internet connections (TCP and UDP) and Active Local Unix domain sockets (stream and datagram)	✓	✓
Screen - Screen Capture	Collect a screenshot of all system displays	✓	
System - Application List	Collect all applications (ending in .app) in the system *Applications* directory	✓	
System - Date	Collect current system date, time, and time zone	✓	✓
System - Environment Variables	Collect environment variable information Collect printenv command return values (sudo user, default shell, current user home directory path, etc.)	✓	✓

Option	Description	Mac	Windows
System - Free Disk Space	Collect free disk space statistics for all mounted file systems	✓	✓
System - Host Name	Collect the computer's localhost name	✓	✓
System - I/O Kit Registry	Collect I/O Kit registry information	✓	
System - NVRAM Variables	Collect all firmware variables for Non-volatile RAM (NVRAM)	✓	
System - OS Version	Collect the operating system software version	✓	✓
System - Open Files	Collect a list of open files	✓	✓
System - Print Jobs	Collect print queue status	✓	✓
System - Printer Status	Collect cups printer status	✓	
System - Processes	Collect active system processes	✓	✓
System - Profile	Collect data about this computer, such as found on these windows: • About this Mac • About, on Windows	✓	✓
System - Scheduled Tasks	Collect list of startup programs	✓	✓
System - Startup Programs	Collect a list of programs launched at startup	✓	✓
Users - Active	Collect a list of local and/or remote users who are currently logged into the computer	✓	
Users - All	Collect a list of user account information	✓	✓

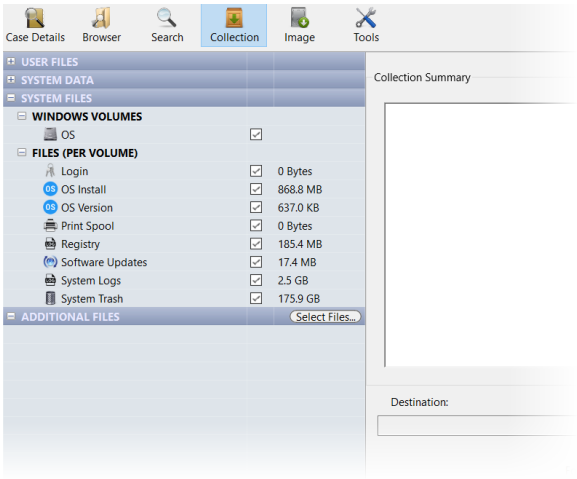
Selecting System Files

Cellebrite Digital Collector allows you to select and collect operating system files and artifacts on all internal or attached volumes. Many volume-specific system files contain valuable forensic information that is often overlooked or forgotten during collection and examination.

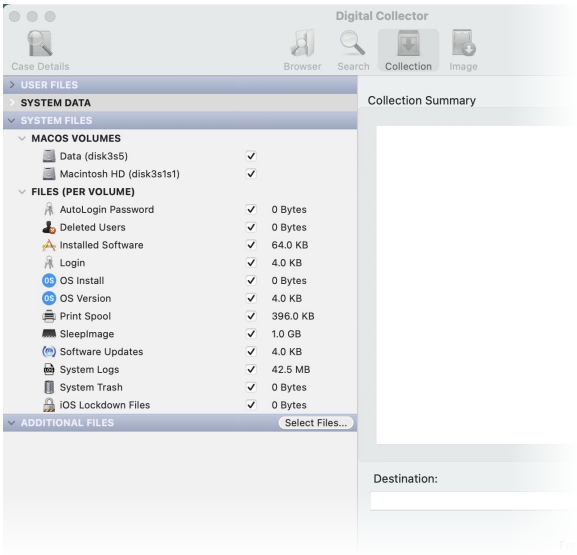
Tip: You can select or deselect everything in the entire list in the Collections view by using the context menu (right-click anywhere in the list) and choosing the appropriate action.

In the toolbar, click **Collection** and then expand the **SYSTEM FILES** section of the list one the left side of the Collection view.

The SYSTEM FILES section of the list looks like this on Windows computers.



The SYSTEM FILES section of the list looks like this on Mac computers.



There are two sections within the SYSTEM FILES section of the list.

- <PLATFORM> VOLUMES, where PLATFORM is either MACOS or WINDOWS
- FILES (PER VOLUME)

These two sections of the list work together.

1. In the <PLATFORM> VOLUMES section, mark the checkbox to the right of each volume that contains data of interest.
2. In the FILES (PER VOLUME) section, you must then mark the checkbox to the right of each item collect for the selected volumes.

For example, you could select two of three possible volumes, and then select only Login, System Logs, and System Trash. The collection is then limited to only the selected items for the selected volumes.

Look in the **Collection Size** field at the bottom of the Collection view, to the right of the list. If you deselect a volume or select another volume, or if you deselect an item or select another item, the size of the collection is recalculated to reflect excluding or including the selected items for the selected volumes. When time is limited, you can quickly triage volume data and system files according to importance. The larger the size, the longer it will take to collect.

Options for Collecting System Files

These are the preset options for system file items that can be collected.

Option	Description	Mac	Windows
AutoLogin Password	Collect the *kcpassword* file if it exists	✓	
Login	Collect lock screen files		✓
Deleted Users	Collect deleted user preference files containing deleted user information	✓	
Installed Software	Collect the system preference containing a list of installed software	✓	
Login	From macOS, collect the */Library/Preferences/com.apple.loginwindow.plist* file (which contains login information for the last user account that was logged into the system, and which may contain guest account login artifacts). From Windows, collect any folders with a path like this: *Windows\SystemApps\Microsoft.LockApp_** These are associated with lockapp.exe, which is responsible for drawing part of the lock screen on Windows 10.	✓	✓
OS Install	Collect operating system install information and date	✓	✓
OS Version	Collect operating system version information	✓	✓
Print Spool	Collect printer cache and print spool information	✓	✓
Registry	Collect system registry		✓

Option	Description	Mac	Windows
SleepImage	Collect the file containing the last laptop macOS system state prior to a drained battery-induced system shutdown	✓	
Software Updates	Collect Software Update application history	✓	✓
System Logs	Collect operating system log files	✓	✓
System Trash	Collect data contained in the system *Trash* folder or the *Recycle Bin*	✓	✓
iOS Lockdown Files	Collect locked iOS device escrow keys (iOS PIN/passcode)	✓	

Selecting Additional Files and Folders

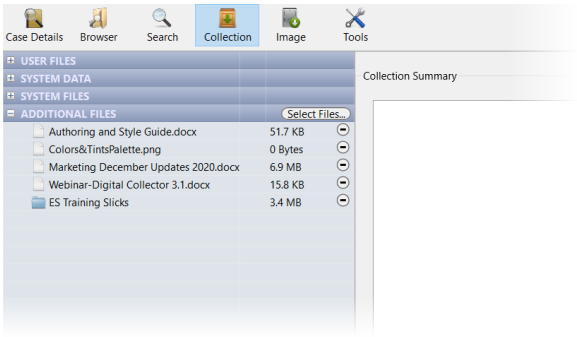
Cellebrite Digital Collector allows you to select and collect files and folders according to specific case requirements. These are typically files you select during triage on the Browser and Search views. For more information, see Browser View and Search View.

These files appear in the Collection view in the ADDITIONAL FILES list.

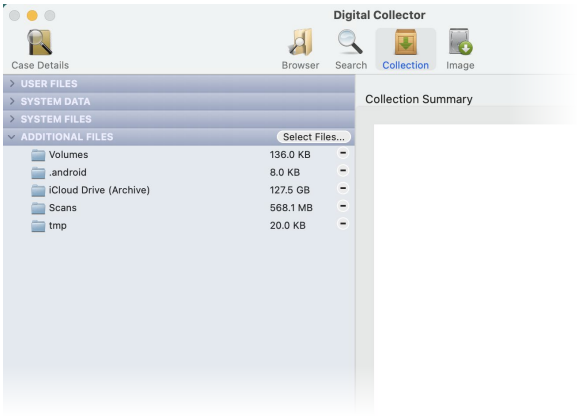
Tip: You can select or deselect everything in the entire list in the Collections view by using the context menu (right-click anywhere in the list) and choosing the appropriate action.

In the toolbar, click **Collection** and then expand the **ADDITIONAL FILES** section of the list on the left side of the Collection view.

The ADDITIONAL FILES section of the list looks like this on Windows computers.



The ADDITIONAL FILES section of the list looks like this on Mac computers.



In the ADDITIONAL FILES list, you can see all folders and files you selected in the Browser or Search views. While you may select more items directly from this list, the Browser and Search views are recommended.

1. To the right of ADDITIONAL FILES, click **Select Files**.
2. In the Files and Folders Selection dialog box, navigate to the appropriate files and folders and then click **Select**.
   If you cannot see or select items, you should instead select them from the Browser or Search views.

To remove a file or folder from the ADDITIONAL FILES list, click **-** (**Remove**) next to the item's name.

Collecting Selected Data

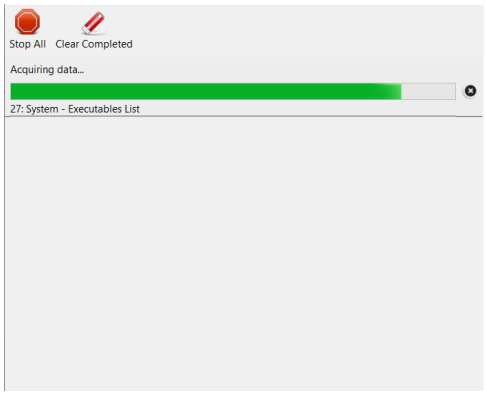
Cellebrite Digital Collector lets you choose the destination for a collection, choose the file format for the collection, specify segmentation, and select hash values to compute.

Before you begin:

- Be sure the destination volume has enough room to hold the collection. The Digital Collector solid state drive (SSD) has a storage volume, *DCData*, which is formatted exFAT. If space is not sufficient in the *DCData* volume, you should connect an additional device for storage. For more information, see Digital Collector Device and Other Equipment.
- Be sure the destination volume is mounted Read/Write. For more information, see Mount Device Tool.
- If the format of the destination will be a folder, be sure that the file system of the destination is the same type as on the source computer. This preserves the most metadata. For more information, see Digital Collector Device and Format Device Tool.

Set the Destination for a Collection

1. When you have finished choosing what needs to be collected, click **Set** to the right of the Destination field, below the Collection Summary on the Collection view.
2. Choose the destination for the collection.
   If the source is a Mac computer booted from the Digital Collector SSD, you may see this message: **`iCloud Drive may not work properly.`**
   Click **OK** and continue with choosing the destination.
3. In the **Format** field, choose the format for the collection.
   - Folder (Available only for Mac computers.)
   - L01
4. In the **Segment Size** field, set the size of the segments for an L01 collection.
   You can choose a size or set a custom size.
5. In **Hashes**, mark the checkbox for any verification hashes to compute for this collection, and then click **Start**.
   The Activity window appears, showing the progress of the collection.



When the collection is complete, the Activity window shows the destination drive, path, and file name.

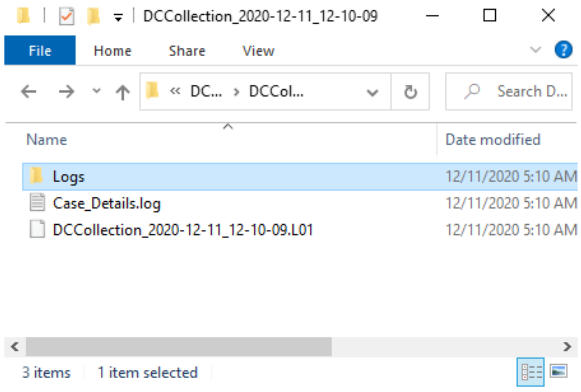
Verifying Collected Data

After data collection is complete, the destination volume contains these files and folders.

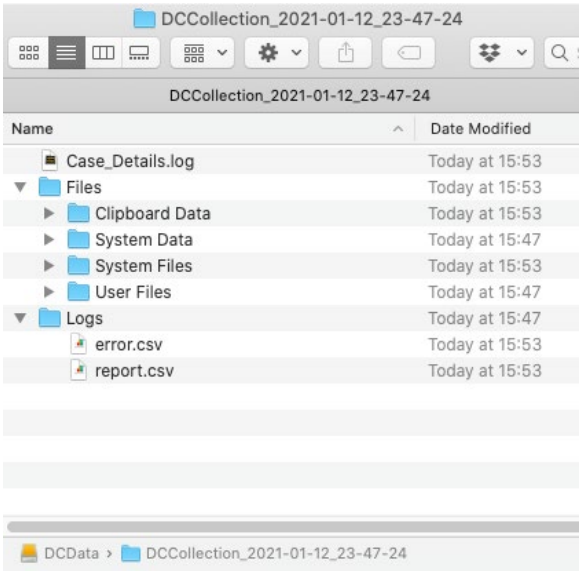
- If the collection is saved to a folder, you see a *Files* folder, a *Logs* folder, and a *Case_Details.log* file.
- If the collection is saved to an L01 file, you see a *Case_Details.log* file. A *Logs* folder is created but has no contents.

You can see the destination volume using File Explorer on Windows computers or Finder on Mac computers.

This is an example of the destination volume on a Windows computer for an L01 collection.



This is an example of the destination volume on a Mac computer for a folder collection.



Files Folder

The *Files* folder is created when the destination is a folder, but not an L01 file.

The *Files* folder contains all the collected data in subfolders. Folders inside the *Files* folder have names that correspond to each section of the list in the Collection view such as System Data, User Files, and so forth. If the Clipboard Data option was selected, there is also a subfolder named *Clipboard Data* that contains a text file with the source computer's clipboard contents.

The folders inside the *Files* folder are only created if you select at least one item in the corresponding section of the list on the Collection view. For instance, if nothing is selected in the ADDITIONAL FILES section, there is no *Additional Files* folder inside the *Files* folder after collection is complete.

Logs Folder

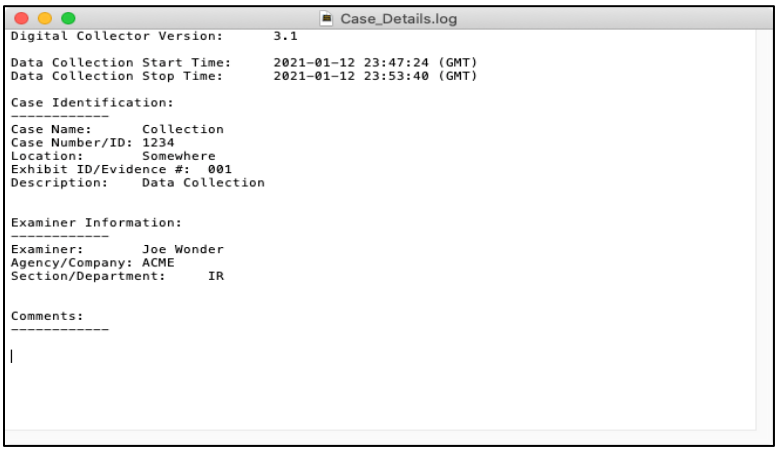
When the destination for the collection is L01, the *Logs* folder is empty. The *Logs* folder contains comma-delimited report files. These files contain very detailed file status information for each collected item, including item collection start and stop times, the item's source path (where the item was on the suspect's computer), destination collection path (the item's *Data Collection/Files* folder location), pre- and post-collection hash values (MD5, SHA-1, and SHA-256), and whether or not the collected item was an alias or hidden file (status on both the source and destination respectively).

These are the report files in the *Logs* folder.

- *report.csv* contains status information for all files collected (does not contain task-based output such as system information, and so forth).
- *error.csv* contains informational and error messages for items that could not be collected.

Case_Details.log File

The *Case_Details.log* file contains collection start and stop times and any information that an examiner entered in the Digital Collector Case Details window before collection started.



Creating an Image

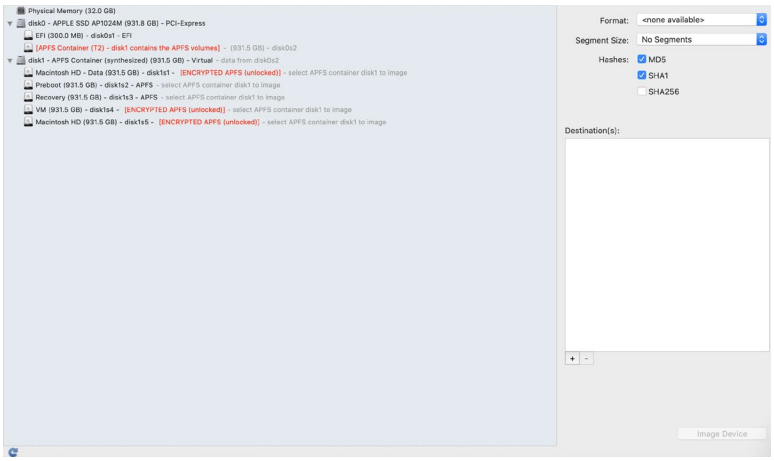
With Cellebrite Digital Collector, you can create an image of entire hard drives and storage devices as well as individual volume partitions.

You can create an image of a source computer that is started (booted) from the Digital Collector solid state drive (SSD). For more information, see Starting a Computer with Digital Collector.

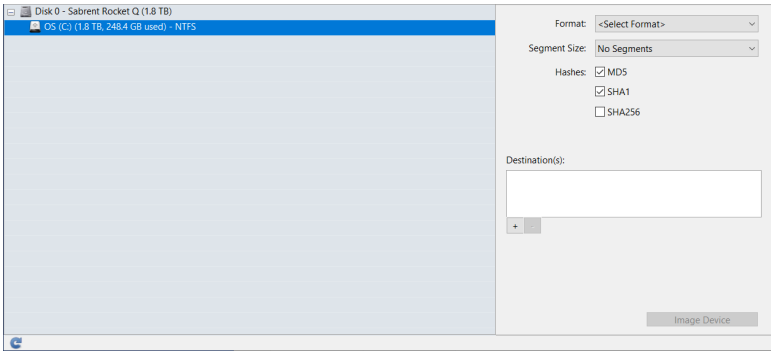
You can also create an image of a device or device partition that is attached to your live host computer. For Mac computers, you can create an image of live APFS volumes that are mounted read/write.

On the toolbar, click **Image**. The Image view appears.

This is an example of the Image view on a Mac computer.



This is an example of the Image view on a Windows computer.



On the left side of the Image view, you can select the source drive or storage device. Device volumes or partitions are shown below their associated hard drive or storage device.

On the right side of the Image view, you can choose settings for the destination of the image, including the hashes.

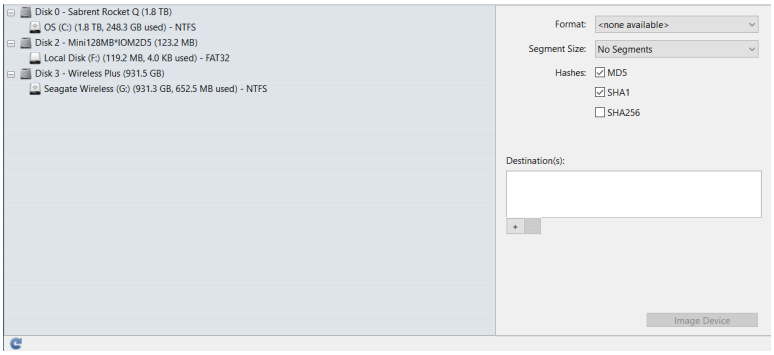
These topics provide details about creating an image using Digital Collector.

- Imaging Windows Computers
- Imaging Mac Computers
- Verify Image Creation

Imaging Windows Computers

You can acquire a physical or logical image of data from a source computer. If the source is a physical device, Digital Collector can create a bit-by-bit forensic image. If the source is a logical slice or partition, Digital Collector can create a bit-by-bit forensic image. This flexibility allows you to quickly acquire targeted data if a full forensic image is not necessary or if time is limited.

To create an image of a Windows computer, click **Image** in the toolbar.



All devices formatted with a recognizable file system are listed in the left side of the Image view. Device icons appear according to the type of each device. You can expand the list for any physical device that contains slices or partitions.

This is the information you can see in the Image view.

- internal physical hard drive (disk0)
- connected storage devices

You can choose the image format, the size of image segments, the hashing, and the destination. The more hash function options you choose, the longer it will take to create the image. If time is limited, you should select only the necessary options.

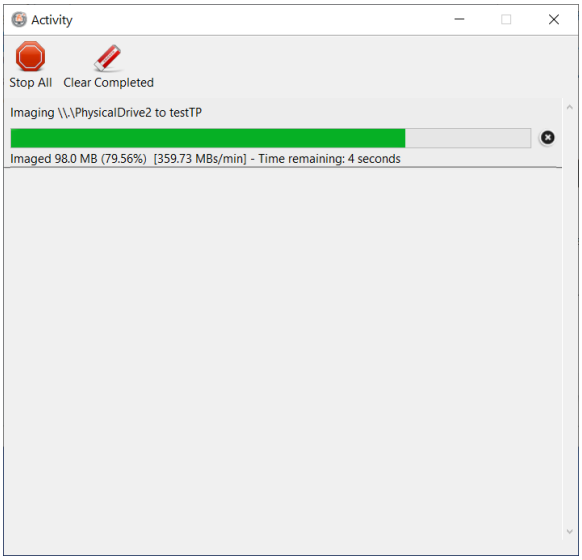
If you formatted the *DCData* partition with NTFS, you cannot write to the *DCData* partition from a Windows computer started from the Digital Collector SSD. You can either format the *DCData* partition to exFAT or, if you must write to a destination formatted NTFS, you can use your own storage device as the destination.

If you select an E01 image format, an image may be acquired onto no more than two destination volumes or folders. An E01 image will contain the MD5 and SHA-1 hash value within the image if these hash options are selected.

The RAW image format does not store the hash value within the image. If you select the RAW image format, an image may be acquired to unlimited destination volumes or folders.

Create an Image of a Windows Computer

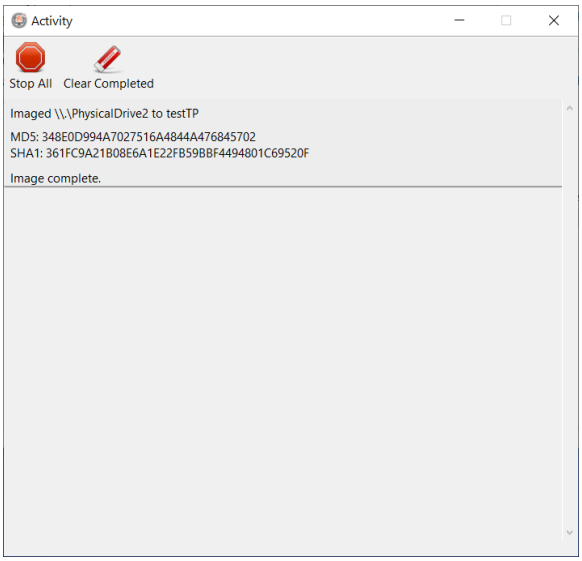
1. On the left side of the Image view, select a device or a partition as the source.
2. In the **Format** field, choose the appropriate option.
   - RAW
   - E01 (Uncompressed)
   - E01 (Empty Block Compression)
   - E01 (Fast Compression)
   - E01 (Best Compression)
3. In the **Segment Size** field, select the appropriate size of segments for this image or specify a custom segment size.
   You may leave this set to No Segments.
4. For **Hashes**, mark the checkboxes for the hash verification values to calculate for this image.
   - MD5 (Message Digest 5)
   - SHA1 (Secure Hash Algorithm 1)
   - SHA256 (Secure Hash Algorithm 2, 256-bit length)
5. Below the bottom left corner of the **Destination(s)** list box, click **+ (Add)** to add a destination volume or folder.
   To remove a destination, select the folder or volume name in the **Destination(s)** list box and click **- (Remove)**, or press DELETE.
6. To create the image, click **Image Device**.
7. Type the name of the image that will be created, and then click **Continue**.
   If there is not enough available space in the destination, a message indicates how much space is available on the destination drive and the space required to successfully acquire the image from the source. Digital Collector does not estimate the size of a compressed image. Take this into consideration and proceed with caution.
   The Activity window and the Imaging in progress banner appear.



The Activity window indicates progress in terms of bytes complete, percentage complete, and estimated time remaining. If you need to step away from the source machine during acquisition,

you can type a custom message in the **Comments** field on the Imaging in progress banner to remind you of what Digital Collector is doing.

Hashes are computed after the image is created. The hash values appear in the Activity window and are also stored in the *Acquisition Log.txt* file, which is created in the image destination folder.



Imaging Mac Computers

Cellebrite Digital Collector detects all connected computers, drives, and storage devices formatted with a recognizable file system, and lists them in the left side of the Image view. Icons appear according to the type of each device. You can expand the list for any physical device that contains slices or partitions.

This is the information you can see in the Image view.

- source system physical memory (RAM)
- internal physical hard drive (disk0)
- internal CoreStorage logical volume (disk1)
- external USB device (disk3)
- APFS Disk Image (disk4)
- APFS Container (disk5)

Slices and partitions are shown below the corresponding physical device. The slice or partition icon indicates file system type and content.

These are the types of physical devices.

Icon	Drive Type
	Internal Hard Drive
	External USB Device
	External FireWire Device
	RAID Array

These are the types of logical devices.

Icon	Drive Type
	EFI or undefined Slice/Partition
	Windows File System
	Apple File System
	Apple Memory
	Apple Core Storage For more information, see these topics: • Unlocking and Imaging CoreStorage FileVault 2 Volumes • Imaging CoreStorage Fusion Volumes • Imaging Single Disk (default) CoreStorage Volumes

Imaging Considerations for macOS

This topic identifies capabilities and constraints in specific circumstances for macOS versions supported by the most recent version of Digital Collector.

Cellebrite cannot ensure that Digital Collector will run properly on initial versions of major macOS releases, such as 12.0. or 12.1. Support is generally declared by the time later versions are released, such as 12.2.

M1 Mac Computers

Digital Collector is supported on M1 computers running macOS 11 and 12.

You can create images of source M1 Mac computers running macOS 11 and 12 either running live or when started from the Digital Collector SSD (booted from the *DC ARM* volume). To see the boot environment on M1 computers, you must hold down the power button until it appears. This may take many seconds. You may then be prompted to do one of these actions:

- Select a user account that can unlock the operating system disk and provide a password for that account.
- Provide the iCloud email address and password of a user that can unlock the operating system disk.

You can image live APFS volumes that are mounted read/write. (A KEXT is no longer required.) During this process the volume is locked/frozen. This can cause behavior that seems unusual until imaging is complete.

Note: Before you begin, you must ensure that the disk being imaged will not try to shut down, has an uninterrupted supply of power, and that the screen never goes to sleep. If you don't take these precautions, you may not see the notification that the image is complete or the image may fail to complete.

Note: To create an image while Digital Collector is running live on macOS 12 Monterey, you must first disable System Integrity Protection (SIP). You can search online for instructions.

Under rare conditions when creating an image (due to an Apple bug), the last few blocks may be allocated and not readable. This failure is detected early in the imaging process and an explanation is written to the error log along with the suggestion that you should instead acquire a logical data collection.

Some volumes in a macOS APFS container may unavoidably be mounted read-write. Digital Collector automatically remounts those volumes as read-only. This action does trigger an innocuous write on the computer being imaged, such as to a log file.

- On macOS 11, the pre-boot and main data volumes are affected.
- On macOS 12, only the main data volume is affected.
- Volumes created by the user, both within the operating system APFS container and in newer user-created APFS containers, are affected.

Due to NTFS driver limitations on newer versions of macOS, Digital Collector cannot write to an NTFS-formatted drive. Previous versions of Digital Collector (including Legacy 2019) have full NTFS support. These legacy boot versions are available on the Digital Collector device.

Be aware of possible constraints with the specific circumstances described here.

Big Sur 11

If the computer is running macOS 11.2, the user interface may respond very slowly. (M1 Macs running macOS 11.4 and later are not affected.)

In rare cases, computers running macOS 11.0 or 11.1 may not start from Digital Collector's boot environment. If this happens, connect the Digital Collector SSD to the subject computer while it is running live or use Disk Sharing Mode.

APFS and All Types of Hardware Encryption

The workflow for imaging APFS volumes with all types of hardware encryption (T2 or M1) is consistent and requires unlocking from within Digital Collector.

1. In the Image view, determine whether there are encrypted volumes that you do or may have a password for.
2. For each of those volumes, click **Tools > Mount Device**, unlock the volume, and then mount it.
3. In the Image view, select the device and click **Image Device**.

File Systems, T2, FileVault 2

This chart can help you determine which device should be imaged, and when FileVault 2 must be unlocked before creating images. The actual disk numbers may differ from this depending on the specific circumstances for acquiring each image.

- Parent physical disk is typically disk0
- Operating system APFS container disk is typically disk1
- Operating system APFS Fusion container disk (merged data from disk0 and disk1) is typically disk2

File System/ T2	Fusion	FileVault 2 Enabled	Imaging
HFS Plus	No	No	Image parent physical disk.
	Yes	No	Image operating system APFS Fusion container disk.
	No	Yes	Image parent physical disk.
	Yes	Yes	1. Unlock encrypted FileVault 2 data. 2. Image decrypted operating system APFS Fusion container disk.
APFS	No	No	Image parent physical disk. (Required if Bootcamp is present.) or Image operating system APFS container disk.
	Yes	No	Image operating system APFS Fusion container disk.
	No	Yes	Image parent physical disk. [1]
	Yes	Yes	Image operating system APFS Fusion container disk. [1]
APFS T2 chip	No	No	Image operating system APFS container disk. [2]
	Yes	No	Image operating system APFS Fusion container disk. [2]
	No	Yes	1. Unlock encrypted FileVault 2 data. 2. Image operating system APFS container disk. [2]
	Yes	Yes	1. Unlock encrypted FileVault 2 data. 2. Image operating system APFS Fusion container disk. [2]

[1] On APFS computers without a T2 chip, FileVault 2 encrypted data can be decrypted later, during analysis with Inspector.

[2] On computers with a T2 chip, you must provide a user login and password or Recovery Key during acquisition.

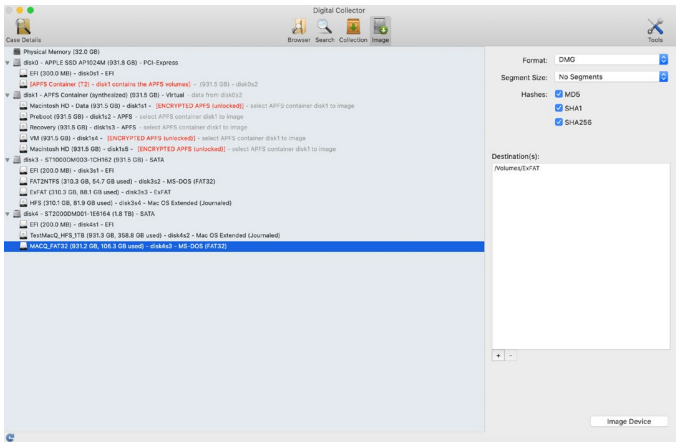
Acquire a Physical or Logical Image of a Mac Computer

You can create images of connected computers, drives, and storage devices. You can also create images of live APFS volumes that are mounted read/write. During this process the volume is locked/frozen. This can cause behavior that seems unusual until imaging is complete.

Note: Before you begin, you must ensure that the disk being imaged will not try to shut down, has an uninterrupted supply of power, and that the screen never goes to sleep. If you don't take these precautions, you may not see the notification that the image is complete or the image may fail to complete.

Note: To create an image while Digital Collector is running live on macOS 12 Monterey, you must first disable System Integrity Protection (SIP). You can search online for instructions.

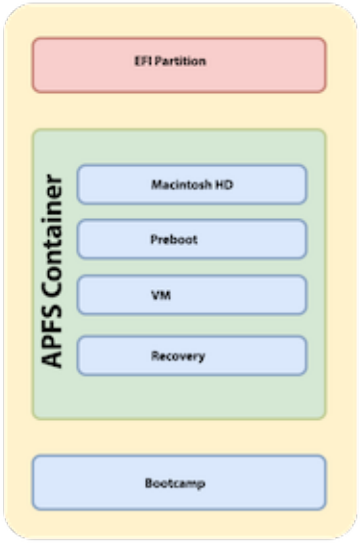
1. On the Digital Collector toolbar, click **Image**.



2. On the left side of the Image view, select a device or device partition.
   If the source device is a physical device, Digital Collector can create a bit-by-bit forensic image. If the source device is a logical slice or partition, Digital Collector can create a bit-by-bit forensic image. CoreStorage Logical Volumes include both allocated and unallocated space. This flexibility allows you to select and quickly acquire data if a full forensic image is not necessary or if time is limited.
3. Specify where the image will be saved.
   You can select multiple image destination locations. Below the bottom left corner of the **Destination(s)** list box, click **+ (Add)** to add a destination volume or folder. To remove a destination, select the volume name in the **Destination(s)** list box and click **- (Remove)**, or press DELETE.
   If this computer was started from the Digital Collector SSD, you may see this message: **`iCloud Drive may not work properly.`**
   Click **OK** and continue with choosing the destination.
4. Specify the format for the image.
   If you select the Raw or DMG image format, an image may be acquired to unlimited destination volumes or folders.
   If you select the E01 image format, an image may be acquired to two destination volumes or folders. If you select the E01 image format and more than two destination volumes or folders, you see this message: **`Warning: Too many destinations specified for the selected format.`** In this case, you should remove a destination volume or folder.

Apple File System Considerations

The Apple File System (APFS) replaced Mac OS Extended format (HFS Plus, or hierarchical file system) as the default file system as of macOS High Sierra 10.13. APFS is much different than Mac OS Extended format. APFS does not define a volume; rather it implements a container which can host several volumes in it. APFS was designed for solid state drives, but it can work with traditional drives.



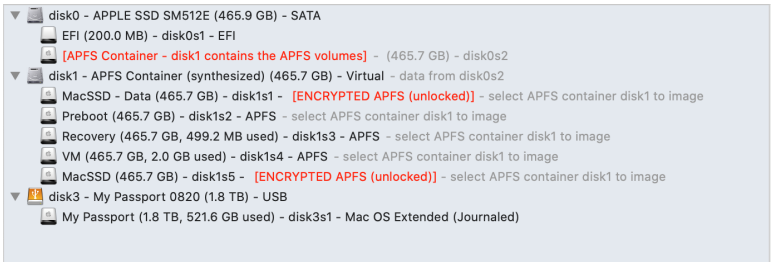
The APFS container by default does not have a limit on the size or location of the volumes within it. Unlike traditional partitions on disk, where sectors are allocated for each volume before they can be used, APFS allows all volumes to share a common pool of extents and they all report having total free space as the same. This also means that data from all volumes is interspersed, and that volumes are not contiguous. Space in the logical container pool can be used by one or more APFS volumes. APFS volumes grow and shrink by allocating unused blocks from the logical container pool and returning those blocks when files are deleted and space is freed. Each APFS container only knows about the blocks used by its own active files, and unallocated space is managed within the logical container pool. Because APFS volumes within a container are not traditional partitions, these volumes in the container cannot be individually imaged.

If you choose to run Cellebrite Digital Collector live on a source computer, keep in mind that on macOS 10.13 and later, while System Integrity Protection (SIP) is active, no user (not even root) can read the physical disk the computer is currently started (booted) from, the physical partition the computer is currently booted from, or the APFS container that holds the currently booted volume. This makes it impossible to image the physical disk. To image, you must either boot the source computer with Digital Collector or attach the source computer in target disk mode (TDM) to another system with macOS 10.13 or later running Digital Collector. For more information, see these topics.

- Start a Mac Computer with Digital Collector
- Connect a Source Mac Computer in Target Disk Mode

If you disable SIP, the APFS container can be imaged when you run Digital Collector on a live source computer. You must authenticate with an admin username and password when you start Digital Collector. For more information, see Imaging Considerations for macOS.

When APFS is encountered, Digital Collector shows an additional device for the APFS container. Digital Collector can image the physical disk device or the synthesized container. When booted to Digital Collector, the physical disk is generally disk0 and the synthesized APFS container is generally disk1.



In this example, the APFS Container shows the volume *Macintosh HD* is locked. This indicates that FileVault 2 is in use; the FileVault Recovery Key or a user account login password is required to unlock the volume for logical data collection.

For Mac computers without the T2 chip, the physical disk should be imaged to capture all data. When the physical disk is imaged, all the data on the device is captured for analysis, including other partitions that are not in the APFS Container. Encrypted partitions within the APFS Container will be imaged in the encrypted state and decrypted during the analysis phase of examination when FileVault 2 credentials are provided.

The APFS Container can also be imaged separately, but the other data on the drive will not be captured.

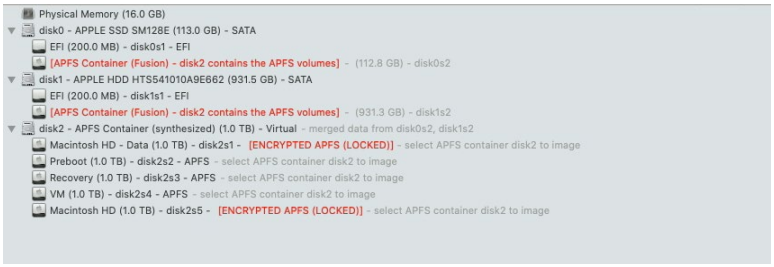
APFS Fusion Drives

With the release of macOS Mojave 10.14, Apple provided an implementation for APFS Fusion drives. The APFS logical container pool may consist of blocks that span across multiple physical partitions. APFS logical containers allow all volumes in the container to share a common pool of extents; data from all volumes is interspersed and volumes are not contiguous. This necessitates an imaging tool that can handle imaging non-contiguous APFS containers. Since synthesized APFS containers do not have a limit on the size or location of the volumes within it, creating a bit-by-bit physical image is not realistic.

Digital Collector performs a physical acquisition that attempts to collect data as it exists on the disks, including data not available through the file system interfaces, providing more options for analysis and recovery of historical or deleted data. A physical image created by Digital Collector can provide access to APFS "Free Queue" blocks, APFS Snapshots, and data hidden in file slack.

To image non-contiguous APFS containers, Digital Collector creates an image using the open standard Advanced Forensic File Format (AFF4) image format. AFF4 is supported by a number of popular forensic tools, including Inspector. It provides modern compression algorithms and the flexibility required to efficiently image non-linear data found on APFS Fusion drives.

When loaded in Digital Collector, the volumes on the physical drives used to create the APFS logical containers are identified with this label, in red: APFS Container (Fusion). The label also indicates the disk of the synthesized APFS container, the volumes used to create the synthesized container, and whether they are locked.



In this example, disk0s2 and disk1s2 form the APFS container. The synthesized APFS container is represented by disk2.

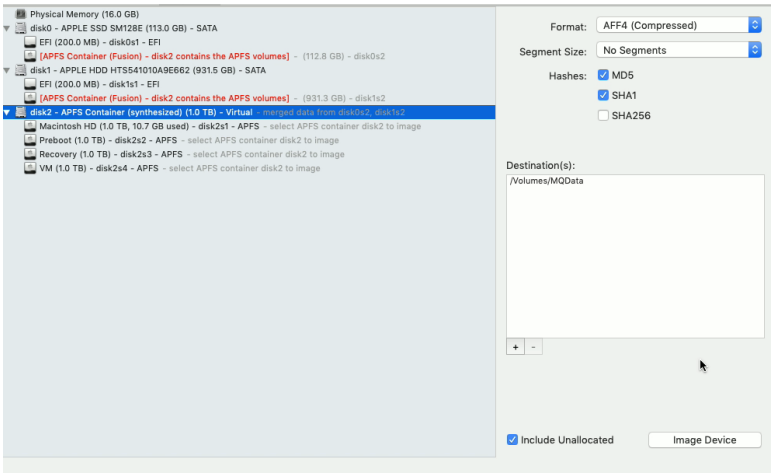
If the physical disk contains other volumes, such as a Bootcamp volume, they must be imaged separately. Any encrypted partitions within the APFS container can be imaged in the encrypted state and decrypted during the analysis phase of examination when FileVault 2 credentials are provided. The encrypted partitions can also be unlocked before acquisition to perform a logical data collection.

The APFS container indicates the disks and partitions used to create the synthesized container and whether they are locked.

Image an APFS Fusion Drive

Encrypted containers do not have to be unlocked before you create a physical image of an APFS Fusion drive. The destination file system cannot be formatted FAT32 due to file size limitations. The image can only be saved to a single destination because AFF4 images cannot be segmented.

1. On the Digital Collector toolbar, click **Image**.
2. Select the disk that represents the synthesized APFS Container (disk2 in this example).



3. Choose the AFF4 image file format, either uncompressed or compressed.
4. Choose the appropriate hashes.

Note: Pre-hashing is not valid for APFS Fusion drives because they are synthesized containers, so you cannot create a bit-by-bit physical image. If **Compare hashes before and after imaging** is selected in the Preferences window, this warning message appears: `Verify Hashes is incompatible with AFF4 imaging`.

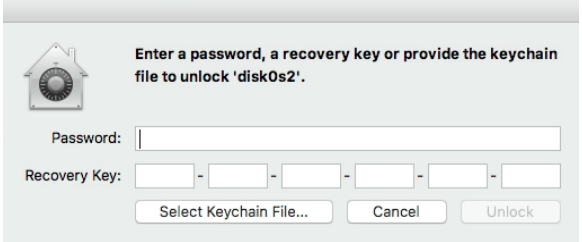
5. Below the bottom left corner of the Destination list box, click **+ (Add)** to add the destination volume or folder.
6. If you want the image to include unallocated space, mark the **Include Unallocated** checkbox.
7. Click **Image Device**.

Hashes selected on the Image view are computed after the image is created. The hash values appear in the Activity window and are stored in the *Acquisition Log.txt* file created in the image destination folder.

Unlock an APFS Fusion Drive

Encrypted containers must be unlocked before you can collect targeted data.

1. On the Digital Collector toolbar, click **Tools > Mount Device**, and then select the locked volume.
2. In the bottom right corner of the Tools view, click **Unlock Selected Device (Read Only)**.



3. Choose the appropriate option to provide credentials to unlock the volume.
   - In the **Password** field, type a password (one of the user account login passwords).
   - In the **Recovery Key** field, type the recovery key.
   - If you are an Enterprise user, click **Select Keychain File**, and then browse to select the *FileVault.keychain* file.
4. Click **Unlock**.
   After the volume is unlocked, the Mount Device tab appears with the volume as read-only.
5. On the Digital Collector toolbar, click **Collection** and select data for a targeted collection. For more information, see Collection View.

Imaging M1 Mac Computers

Creating an image of an M1 Mac is similar to creating an image of a T2 Mac. For more information, see Imaging Mac Computers with T2 Chips.

These are the key points you should be aware of.

- To create an image while Digital Collector is running live on macOS 12 Monterey, you must first disable System Integrity Protection (SIP). You can search online for instructions.
- An M1 Mac may require the password for an admin account when starting from an external drive such as Digital Collector.
- When you start an M1 Mac from Digital Collector, you must hold down the power button for ten seconds to see the boot environment.

  Select **DC ARM Boot** and click **Continue**.

  You may then be prompted to do one of these actions:

  - Select a user account that can unlock the operating system disk and provide a password for that account.
  - Provide the iCloud email address and password of a user that can unlock the operating system disk.
- As with T2 Macs, the Macintosh HD data volume must be unlocked and mounted read-only. Volumes are mounted read-write by the operating system's Recovery Assistant. Digital Collector automatically attempts to unmount any volumes that are read-write. If any data volumes are not mounted, click **Tools > Mount Device** to mount them as read-only.
- Some volumes from the macOS APFS container may unavoidably be mounted read-write. Digital Collector automatically remounts those volumes as read-only. This action does trigger an innocuous write on the computer being imaged, such as to a log file.
  - On macOS 11, the pre-boot and main data volumes are affected.
  - On macOS 12, only the main data volume is affected.
  - Volumes created by the user, both within the operating system APFS container and in newer user-created APFS containers, are affected.
- If iCloud Lock is enabled for the computer, you must provide the iCloud email address and iCloud password.
- If the computer is running macOS 11.2, the user interface may respond very slowly. M1 Macs running macOS 11.4 and later are not affected.

Imaging Mac Computers with T2 Chips

Beginning in 2017, some Mac computers were built with Apple's T2 security chip, which provides hardware-assisted encryption for data stored on the computer. T2 chips are embedded into the disk controller and contain unique encryption keys. Encryption provided by the T2 chips works in conjunction with FileVault 2. When FileVault 2 is enabled, the Recovery Key or password is required to decrypt the data.

By default, all APFS volumes that contain user data on T2-protected computers are encrypted. The only way to decrypt the data is to use information embedded in the T2 chip for its T2-protected computer. Currently, it is not possible to extract encryption keys from the T2 chip. If the T2 chip is damaged, data can never be recovered from the drive.

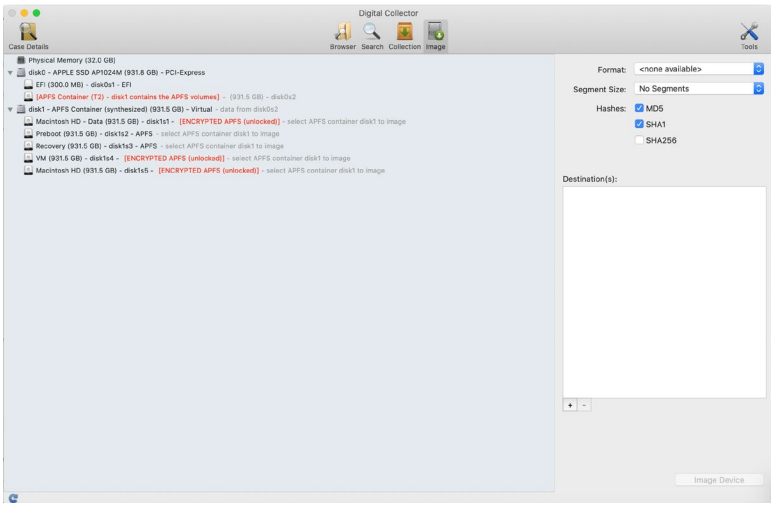
Cellebrite Digital Collector interfaces with the T2 chip to decrypt the file system at collection time, providing a physical image. Since the T2 chip is responsible for all encryption, all data must be decrypted during acquisition; it is not possible to decrypt the data at analysis time. Digital Collector can also decrypt unallocated space. However, research and testing have revealed there is minimal data that remains in unallocated space after deleting files on Mac computers with a T2 chip. To save time, you can enable the option to skip imaging unallocated space.

These are the ways you can acquire decrypted data from a Mac computer with a T2 chip using Digital Collector.

Source Computer	Digital Collector	Requirements and Constraints
Running	Connect the Digital Collector SSD to the source computer obtain a live logical data collection. For more information, see these topics. • Launch Digital Collector on a Live Mac Computer • Collecting Data from a Source Computer	While some user data can be collected without a password, an administrator password is required for full disk access. Cannot acquire an image. Makes changes to the source computer. For more information, see Appendix: Changes to Live Computers.

Source Computer	Digital Collector	Requirements and Constraints
Not running	The most forensically sound method requires a host computer, which must be a Mac computer model from 2012-2019. Put the source computer into target disk mode (TDM), start your host computer with Digital Collector, and connect the source to the host. Creating an image is recommended. Obtaining a logical data collection is useful when you cannot create an image. For more information, see these topics. • Connect a Source Mac Computer in Target Disk Mode • Start a Mac Computer with Digital Collector • Collecting Data from a Source Computer	Does not require an administrator password for the source computer. If Digital Collector detects that FileVault 2 is enabled, you must be able to unlock it. Creating an image requires either the FileVault 2 password or the Recovery Key. Creating a logical collection requires either the FileVault 2 password, the Recovery Key, or the keychain file.
Not running	If you do not have a host computer, change the secure start settings on the source computer, and then use the startup manager on the source computer to start it with Digital Collector. Creating an image is recommended. Obtaining a logical data collection is useful when you cannot create an image. For more information, see these topics. • Start a Mac Computer with Digital Collector • Collecting Data from a Source Computer	Requires an administrator password to change the source computer's secure start settings. If Digital Collector detects that FileVault 2 is enabled, you must be able to unlock it. Creating an image requires either the FileVault 2 password or the Recovery Key. Creating a logical collection requires either the FileVault 2 password, the Recovery Key, or the keychain file.

When a T2 computer is started from Digital Collector, the physical disk displays this label in red: APFS Container (T2).



If the physical disk is imaged (disk0 in this example), the resulting image is encrypted. The information needed for decryption is on the T2 chip, so decryption must occur during acquisition. For Digital Collector to decrypt the macOS data, the synthesized APFS container needs to be imaged. If the synthesized APFS container contains locked volumes, you must enter the FileVault Recovery Key or a user account password to unlock the volume.

- When you obtain a decrypted physical image, unlocking FileVault is built into the workflow after you click **Image Device**.
- When you obtain a decrypted logical collection, you must first unlock FileVault in **Tools > Mount Device**.

If the physical disk contains other volumes, such as a Bootcamp volume (not encrypted), they must each be imaged separately.

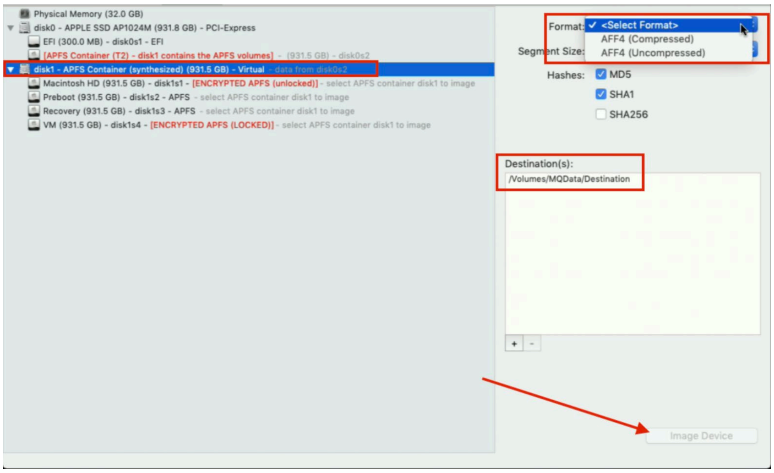
As the APFS container on the computer is acquired, Digital Collector interfaces with the T2 chip to decrypt the T2-protected data, creating a decrypted physical image. Pre-image hashing is not valid because the data is decrypted during the acquisition process. To create the physical image, Digital Collector creates an image using the open standard Advanced Forensic File Format (AFF4) image format. AFF4 provides modern compression algorithms and the flexibility required to efficiently image non-linear data, the APFS container, while optionally skipping data such as the unallocated space.

Important: Digital Collector calculates the hash of the image within the AFF4 container, not of the entire AFF4 file itself. To verify the AFF4 hash, you must use a tool specifically designed for hashing AFF4 images, such as Digital Collector, Inspector, or Evimetry.

Acquire a Decrypted Physical Image of an APFS T2 Container

Unlocking FileVault 2 is built into the Digital Collector workflow for creating a decrypted physical image of an APFS container. Using the Mount Device tool in Digital Collector independently cannot create a decrypted physical image.

1. In the Digital Collector toolbar, click **Image.**
2. On the left side of the Image view, select the APFS Container.
3. In the **Format** field, choose AFF4 (Compressed) or AFF4 (Uncompressed). AFF4 images cannot be segmented. They can only be saved to one destination and cannot be saved to FAT32 formatted drives due to file size limitations in FAT32.
4. In **Hashes**, choose the appropriate hash types. Hashes selected on the Image view are calculated after the AFF4 image is created.
5. Below the bottom left corner of the Destination list box, click **+ (Add)** to add a destination volume or folder.



6. To save time by excluding unallocated space from the image, unmark the **Include Unallocated** checkbox.

7. Click **Image Device**.
8. If FileVault 2 is enabled, a FileVault 2 message appears.
   You must provide credentials to unlock the volume. Choose one of these actions.
   - If you have account credentials for this computer, type the password in the **Password** field.
   - If you have the recovery key for this computer, type it in the **Recovery Key** field.
9. Click **Unlock**.

Digital Collector starts creating a fully decrypted physical image.

Unlocking and Imaging CoreStorage FileVault 2 Volumes

If you connect the Cellebrite Digital Collector solid state drive (SSD) to a live source computer and it has an encrypted CoreStorage (FileVault 2) boot volume or attached device, that data is unlocked and accessible.

In the Digital Collector toolbar, click **Image.**

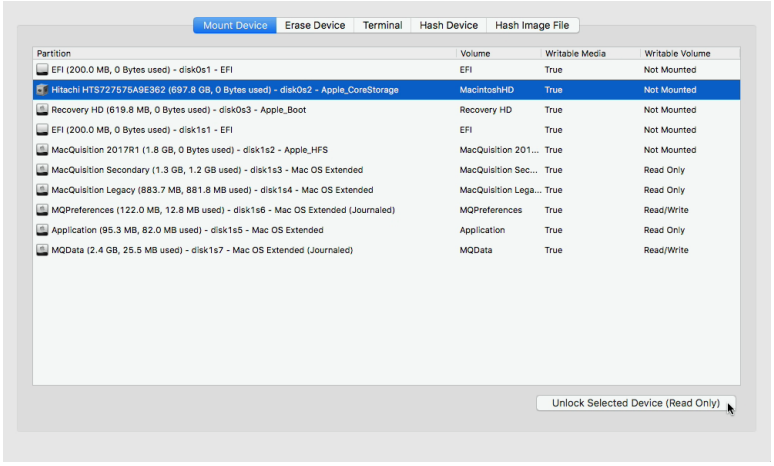
Digital Collector identifies which disk is the decrypted CoreStorage logical volume in red text, for example [ENCRYPTED CoreStorage - disk1 contains decrypted data]. In this example, you would select disk1 to image the decrypted and now readable data.

Warning: Cellebrite recommends performing an extensive live data collection before you shut down the source computer, because once it is shut down, full volume encryption is enabled.

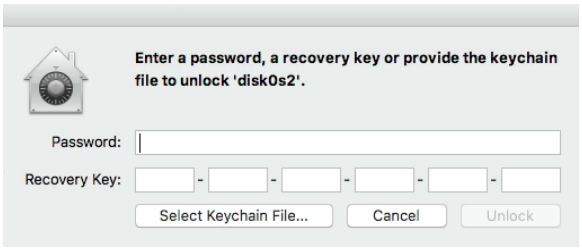
If you know or can recover a boot volume CoreStorage decryption password or decryption Keychain file, a full disk image might be acquired by booting to the Digital Collector SSD and following these instructions.

Unlock a CoreStorage Volume

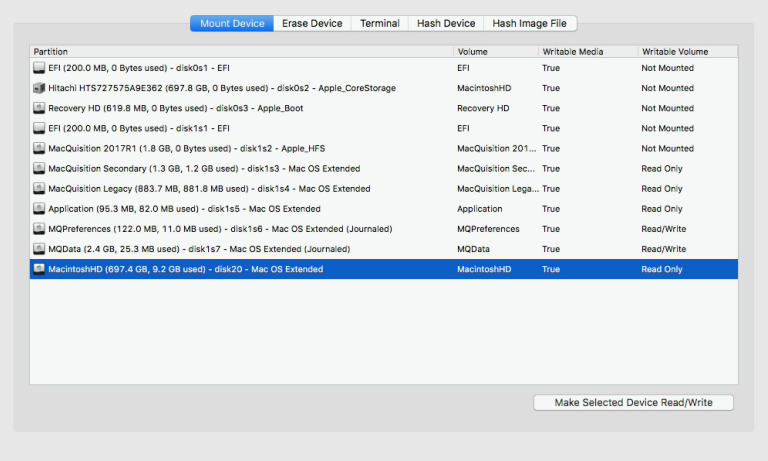
1. To dismiss the full volume encryption warning message and launch Digital Collector, click **Continue**. The Digital Collector window appears.
2. On the Digital Collector toolbar, click **Tools**.
3. Click **Mount Device**, and then select the CoreStorage volume, as shown here.



4. If the source computer is booted to the Digital Collector SSD, click **Unlock Selected Device (Read Only)**.



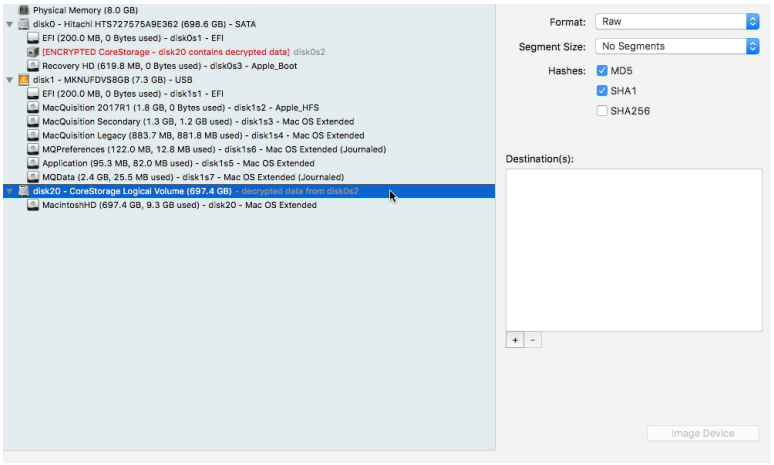
5. Provide credentials to unlock the CoreStorage volume using the appropriate option.
   - In the **Password** field, type a password (often one of the user account login passwords).
   - In the **Recovery Key** field, type the recovery key.
   - If you are an Enterprise user, click **Select Keychain File**, and then browse to select the *FileVault.keychain* file.
6. Click **Unlock**.
7. After the CoreStorage volume is unlocked, the Mount Device tab appears with the decrypted read-only mounted CoreStorage disk. The CoreStorage logical volume mounts as a separate disk after it is decrypted.



Imaging a Decrypted CoreStorage Disk

On the Digital Collector toolbar, click **Image**.

These items related to CoreStorage appear: the encrypted volume and the decrypted logical volume.

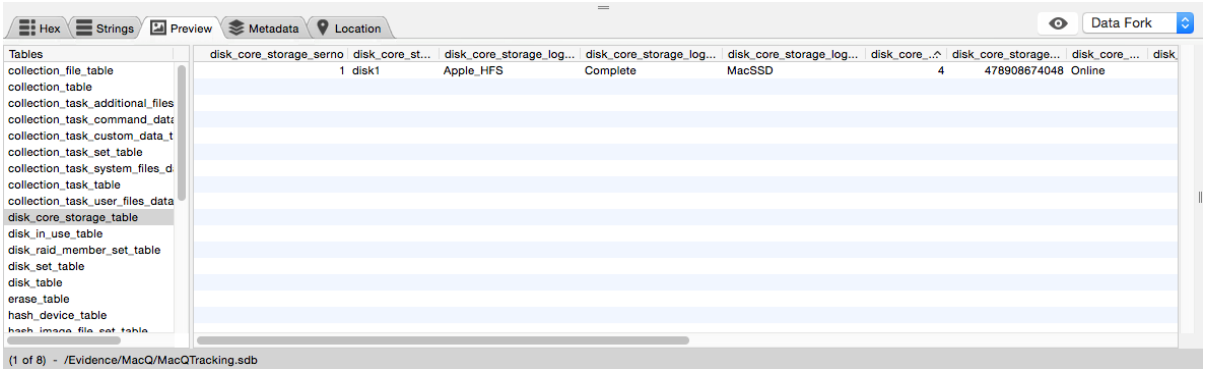


In this example, disk0 contains the encrypted CoreStorage volume. After a CoreStorage volume is decrypted, it mounts as a separate disk. The decrypted CoreStorage logical volume may not appear immediately below the disk containing the encrypted CoreStorage volume. This is due to the Mac operating system dynamically assigning BSD names (disk0, disk1, and so forth) to disks as they are mounted to the file system. Disk0 and disk1 were already mounted to the file system before the CoreStorage volume was decrypted. When the CoreStorage volume was unlocked, the Mac operating system mounted the decrypted CoreStorage logical volume as disk20.

Digital Collector identifies which disk is the decrypted CoreStorage logical volume in red text, as in this example: [ENCRYPTED CoreStorage - disk20 contains decrypted data]. In this example, you would select disk20 to image the decrypted and now readable data.

A CoreStorage logical volume has both allocated and unallocated space.

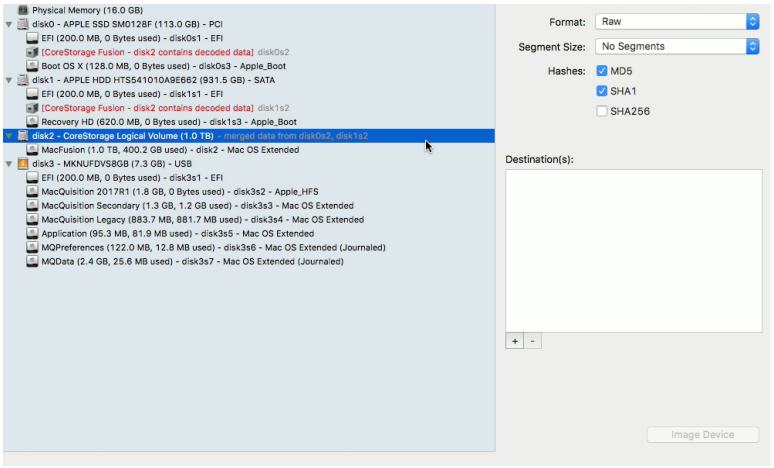
After a decrypted CoreStorage image acquisition is complete, the *disk_core_storage_table* in the *DCTracking.sdb* file contains a CoreStorage acquisition record as seen here (viewed using Inspector).



Imaging CoreStorage Fusion Volumes

Apple's first implementation of CoreStorage was FileVault 2. They went on to use the CoreStorage logical volume manager to create the Fusion Drive, which is a volume capable of spanning two or more physical disks.

Cellebrite Digital Collector identifies Fusion and automatically lists the two or more parent physical disks and presents the Fusion volume as a single CoreStorage-managed logical volume.



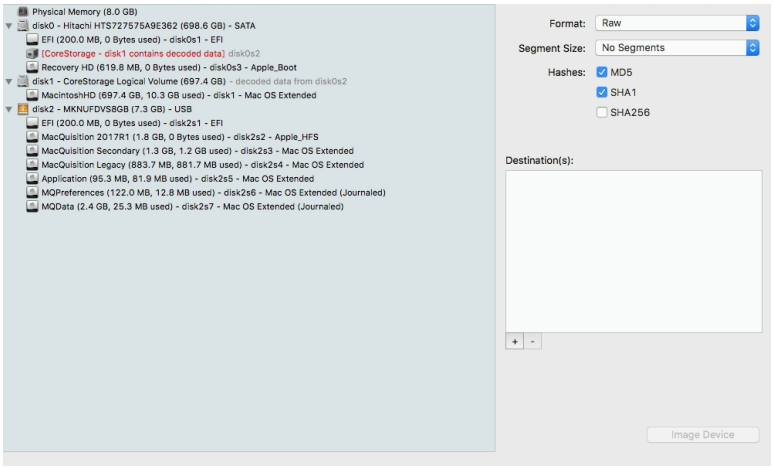
In this example, disk0 and disk1 are the physical disks that contain the spanned Fusion volume. The red text [CoreStorage Fusion - disk 2 contains decoded data] identifies the CoreStorage logical volume that contains the decoded and now readable data. Disk2 is the CoreStorage Logical Volume containing the merged data from both physical disks, disk0s2 and disk1s2. In this example, you would select disk2 to image the combined readable data.

A CoreStorage Logical Volume has both allocated and unallocated space.

When Apple ships a Fusion drive, it is not encrypted. The user may decide later to enable FileVault 2 encryption. For more information about imaging a Fusion drive with FileVault 2 encryption, search for blog posts and videos at https://www.cellebrite.com/en/resources.

Imaging Single Disk (default) CoreStorage Volumes

Some computers with OS X El Capitan 10.11.x and later have a standard CoreStorage volume. Before the release of APFS, this CoreStorage volume was the Mac operating system default for non-FileVault 2 single disk systems. Cellebrite Digital Collector identifies a physical disk that has CoreStorage and presents the CoreStorage logical volume.



In this example, disk0 is the physical disk with CoreStorage. The red text [CoreStorage - disk1 contains decoded data] identifies the CoreStorage logical volume that contains the decoded and now readable data. Disk1 is the CoreStorage logical volume with decoded data. As of macOS 10.12.5, both the physical disk and logical volume of default CoreStorage are decoded and now readable. In this example, you could select either disk0 or disk1 to acquire readable data. Be aware that an image of disk1, the CoreStorage logical volume, will not include the EFI partition or Recovery HD partition, which are contained on disk0, the actual physical disk.

A CoreStorage logical volume has both allocated and unallocated space.

Destination Image File Options

In Cellebrite Digital Collector, you can select the destination image file format (physical bit-by-bit image file or logical acquisition image file).

On the right side of the Image view, click **Format** and choose one of these file types.

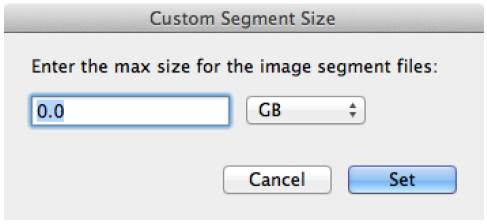
Option	Description
AFF4 (Compressed)*	Create an Advanced Forensic File Format compressed image
AFF4 (Uncompressed)*	Create an Advanced Forensic File Format uncompressed image
Raw	Create a raw or dd image
DMG	Create an Apple disk image
E01 (Uncompressed)	Create an EnCase uncompressed image
E01 (Empty Block Compression)	Create an EnCase compressed image
E01 (Fast Compression)	Create an EnCase compressed image
E01 (Best Compression)	Create an EnCase compressed image

*AFF4 format is only available for APFS containers. AFF4 must be selected for APFS Fusion drives and computers with T2 chips.

For all image formats except for AFF4, you may want to set segment size for the destination image file. This setting determines the size of each destination image file part. For example, if you image a 250 GB hard drive and choose the 4 GB segment size, Digital Collector creates roughly 62 4-GB file parts.

On the right side of the Image view, click **Segment Size** and choose the appropriate size. You can choose any of these sizes, or you specify a custom size in MB, GB, or TB.

- No Segments
- 640 MB
- 1 GB
- 4 GB
- 8 GB
- Custom



Note: It is important to format the destination device appropriately. For instance, if the destination device is formatted with a FAT32 file system, the largest supported acquisition segment size is 3.9 GB. Because AFF4 images cannot be segmented, they cannot be stored on devices formatted with FAT32.

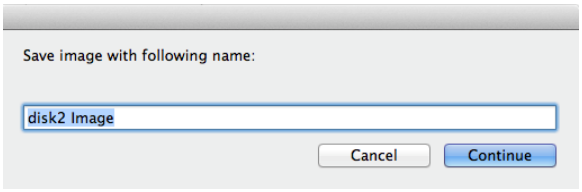
Next, choose hash types for the image. You can mark any or all checkboxes to the left of these options.

- MD5 (Message Digest 5)
- SHA1 (Secure Hash Algorithm 1)
- SHA256 (Secure Hash Algorithm 2, 25- bit length)

The more hash function options you choose, the longer it will take to create the image. If time is limited, you should select only the necessary options.

An E01 image will contain the MD5 and SHA-1 hash value within the image if these hash options are selected. AFF4, Raw and DMG image formats do not store the hash values within the image.

Once you have selected all the necessary destination file options, you can create the image. In the lower right corner of the Image view, click **Image Device**.



Type the name of the image you are creating, and then click **Continue**.

If you launch Digital Collector with restricted permissions but the source computer has admin-only permission settings, a warning message appears. Relaunch Digital Collector and enter an administrator password when prompted.

Note: If you selected RAW, DMG, E01 (Uncompressed), or AFF4 (Uncompressed) format and the destination drive capacity is not large enough, a message indicates how much space is available on the destination drive and the space required to successfully acquire the image of the source computer. Digital Collector does not estimate the size of a compressed image. Therefore, if AFF4 or E01 with compression is selected and the destination drive capacity is insufficient for an uncompressed image, a message indicates how much space is available on the destination drive. Take this into consideration and proceed with caution.

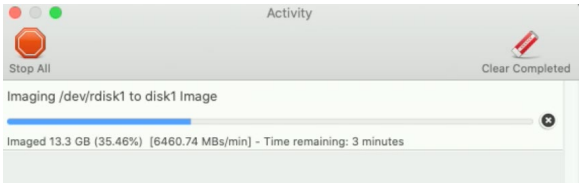
The Imaging in progress bar indicates progress in terms of bytes complete, percentage complete, and estimated time remaining. If you need to step away from the source computer during acquisition, you can type a custom message in the text field.

Hashes are computed after the image is created. The hash values appear in the Activity window and are also stored in the *Acquisition Log.txt* file, which is created in the image destination folder. For more information, see Verify Image Creation.

Activity Window

While an image is being acquired, Cellebrite Digital Collector displays the Activity window. A progress bar indicates bytes complete, percentage complete, and estimated time remaining.

To stop the acquisition process, click **Stop All**, or on the right side of the progress bar click **X**.



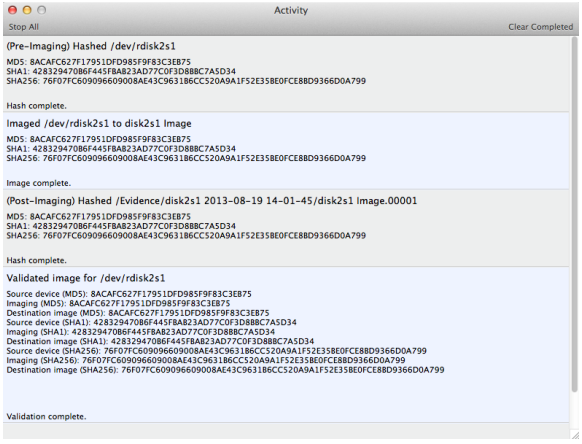
When acquisition is complete, the Activity window shows the acquisition source, the destination, and the MD5 and SHA-1 hash values. If the SHA-256 hash option was also selected, that hash value appears in the Activity window and the *Acquisition Log.txt* file.

Hash Verification

You can hash and verify an image before, during, and after the image is acquired. For more information, see these topics.

- Setting Preferences on a Mac Computer
- Setting Preferences on a Windows Computer

This example shows a post-acquisition Activity window with the verification preference enabled.

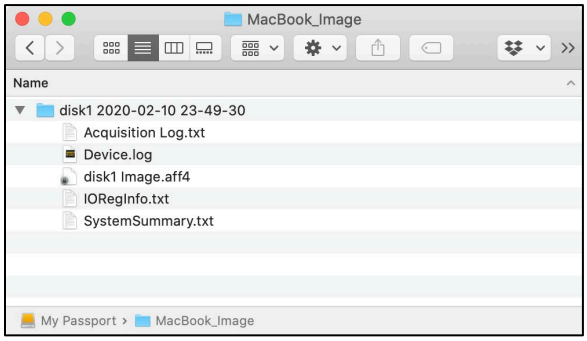


Verify Image Creation

Navigate to the destination image folder. On Mac computers, use Finder. On Windows computers, use File Explorer.

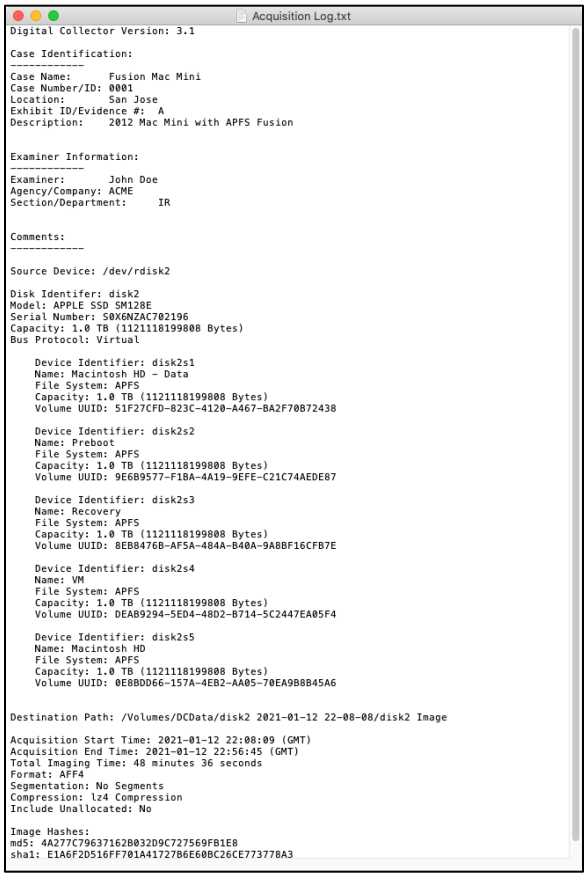
The destination image folder contains a subfolder named with the source device name and the acquisition completion date and timestamp. This folder contains four types of log files and the acquired image file.

In this example, the source device is *disk1*, so the *MacBook_Image* destination folder contains a subfolder named *disk1 2020-02-10 23-49-30*.



Acquisition Log.txt File

The *Acquisition Log.txt* file provides detailed acquisition information and hash values for each hash option selected (MD5, SHA1, SHA256).



If you enable the imaging hash verification preference, the *Acquisition Log.txt* file contains has values for pre-, during-, and post-acquisition. For more information, see Menu Bar.

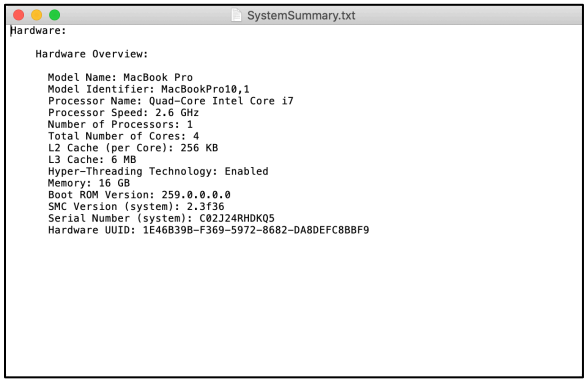
Device.log File

The *Device.log* file contains the **dc3dd** acquisition command that was issued as well as detailed information about the source device, including any errors that may have occurred during the acquisition process for images created with **dc3dd**.

If you select the E01 file format for the destination image file, Digital Collector also creates a *Device.2.log* file. This file contains the hash values that were selected in the Image view.

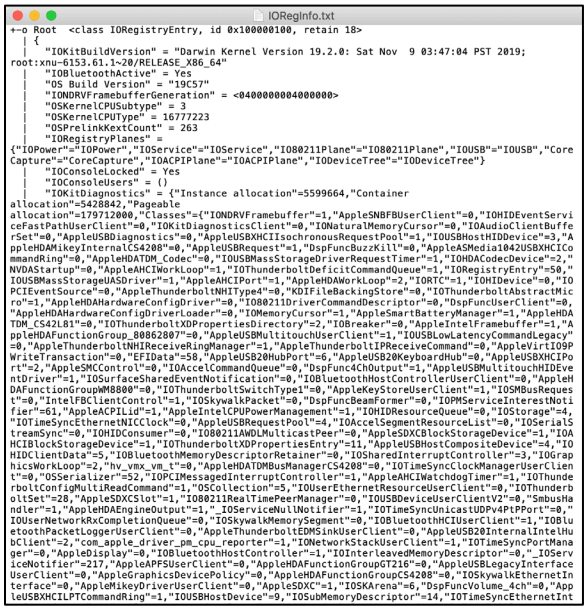
SystemSummary.txt File

The *SystemSummary.txt* file contains the system hardware overview from the **system_profiler SPHardwareDataType** command.



IORegInfo.txt File

The *IORegInfo.txt* file contains output from the I/O Registry using the **`ioreg -w0 -l`** command.



Tools

Cellebrite Digital Collector includes advanced acquisition tools developed for experienced forensic examiners. Some of these tools are only useful when the examiner starts (boots) the source computer from the Digital Collector solid state drive (SSD), as they are unusable or inappropriate during a live acquisition.

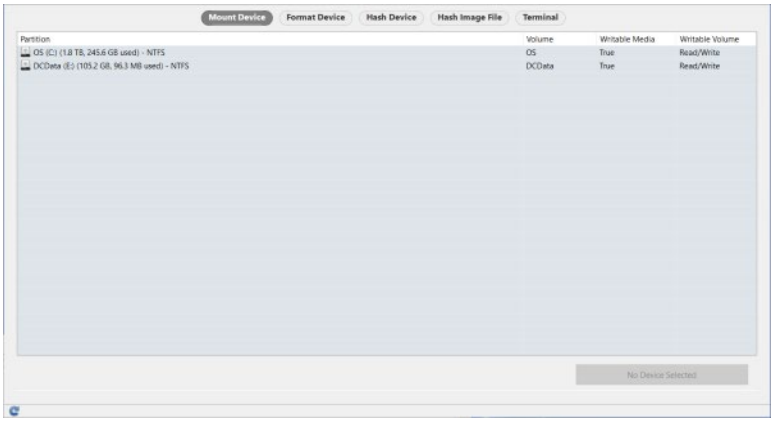
To access these advanced tools, in the Digital Collector toolbar, click **Tools**.

Warning: Use caution when using the Digital Collector advanced tools. Improper use of these tools may result in evidentiary data loss or contamination.

This chapter provides these topics.

Mount Device Tool

When you start (boot) a source computer from the Cellebrite Digital Collector solid state drive (SSD), all source computer internal drives and mounted and attached devices are write protected by default. This means that the operating system on the Digital Collector SSD cannot write to a drive or device unless you change its mount status to read/write. When that is necessary, you can use the Mount Device tool.



When a Mac computer has FileVault 2 enabled, the Mount Device tool can unlock FileVault 2 so that you can create a logical data collection. The Mount Device tool cannot unlock APFS containers for creating physical images.

1. In the toolbar, click **Tools > Mount Device**.
   The Partition list shows all drives and devices. This list also shows attributes such as volume name, capacity, partition or slice name, file system type, a writable media indicator, and the device mount status, including Read/Write or Read Only.

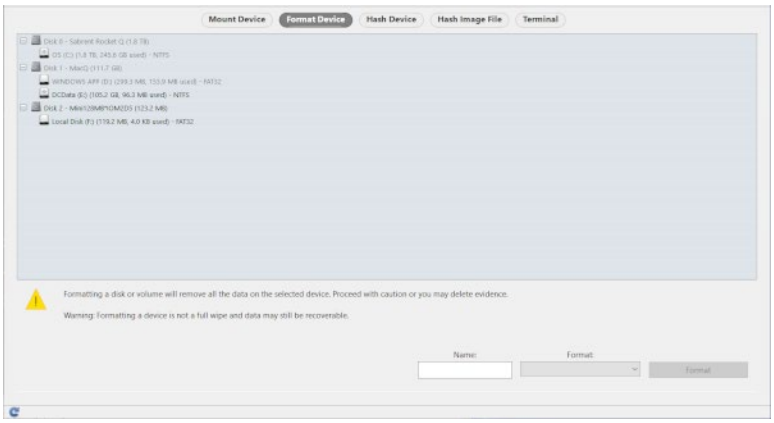
Choice	Action
Mount a read-only device with read/write permissions.	Select the device, and then click **Make Selected Device Read/Write**.
Unlock FileVault encryption on a Mac computer.	a. Select the encrypted volume, and then click **Unlock Selected Device (Read Only)**. b. You must provide credentials to unlock the volume. Choose one of these actions. c. If you have account credentials for this computer, type the password in the **Password** field. d. If you have the recovery key for this computer, type it in the **Recovery Key** field. e. If you are an Enterprise user, click **Select Keychain File** and then browse to select the FileVault.keychain file. f. Click **Unlock**.

2. Read the warning message, and then click **Continue** to complete the mount status change.

Format Device Tool

You can format an entire disk, drive, or device, or a single disk, volume, or partition using the Format Device tool in Cellebrite Digital Collector.

Internal hard drives and attached devices appear in a hierarchical list. Drive and device partitions appear below their associated drive or device. Device icons appear according to the type of device, such as internal, external, FireWire, or external USB. Partition icons appear according to the format of the partition's file system (if a file system exists).



Format an Entire Disk or a Single Volume

1. In the toolbar, click **Tools > Format Device**.
2. Click on the name of the correct internal disk, drive, external storage device, or single volume or partition.
3. In the **Volume Name** field, type the appropriate name for the volume.

   Note: If you are formatting the *DCData* disk, you must ensure it retains the *DCData* volume name.

   Warning: Never format the entire Digital Collector SSD or any volume on the device other than *DCData*. Doing so will require you to reinstall Digital Collector.

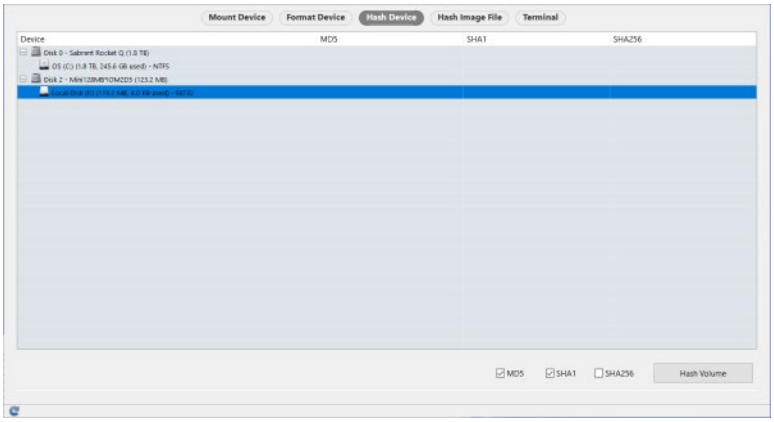
4. Click **Format** and choose the appropriate file system format. You may choose from these file systems:
   - hfsx (Case Sensitive)
   - HFS+ (hierarchical file system plus, also known as Mac OS Extended format)
   - MS-DOS (FAT 32)
   - NTFS (may not be available on Mac computers running with restricted permissions)
   - exFAT (required for the *DCData* volume when the source computer runs Windows and is booted from Digital Collector)
5. Click **Format Volume**.
6. Read the warning message.
   Verify that you selected the correct disk, drive, device, or volume in Step 1 to be sure you do not accidentally format an entire disk if the intention is to erase a single volume.
7. Click **Continue**.
   The volume is named and reformatted.

Hash Device Tool

You may generate hash values for an internal drive, an external device, or a single volume using the Hash Device tool in Cellebrite Digital Collector. You can choose one or all of these options to generate the hash value.

- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)
- Secure Hash Algorithm 2, 256-bit length (SHA-256)

Hard drives and attached devices appear on the Hash Device tab in a hierarchical list. Volumes appear below their associated drive or device. You can expand or collapse the view of volumes. Device icons appear according to the type of device, such as internal, external, FireWire, or external USB. Volume icons appear according to the format of the volume's file system (if a file system exists).



Hash an Entire Drive or a Single Volume

1. In the toolbar, click **Tools > Hash Device**.
   Click the name of an internal drive, or external storage device, or a single volume.
2. Mark the checkbox for any or all of the hash options, and then click **Hash Entire Disk** or **Hash Volume**.
   The Activity window shows hash progress expressed as hashed data complete, percentage complete, hashing speed (MBs/min), and estimated time remaining.
   To stop a hash process, click **Stop All**. Read the warning message, and then click either **Continue Activity** or **Stop Activity**.

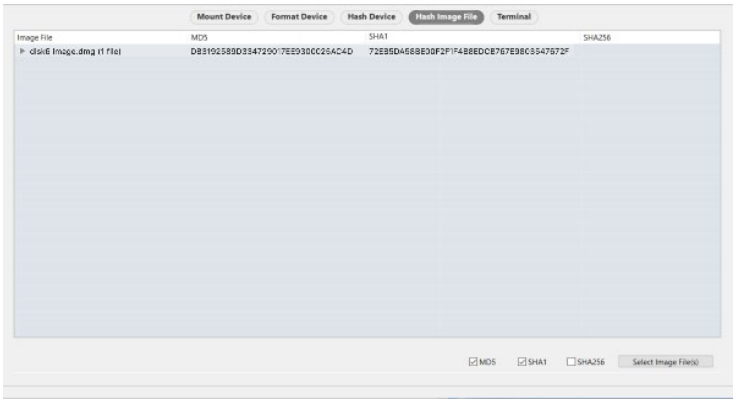
When the hash process is complete, selected hash values appear in the Activity window and in the Hash Device tool window under the appropriate column according to hash type.

Hash Image File Tool

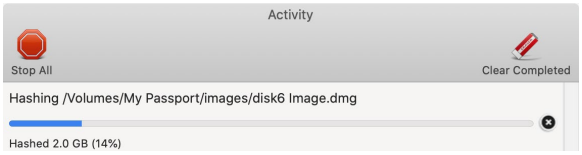
You may generate hash values for one or more forensic image files using the Hash Image File tool in Cellebrite Digital Collector. These are the supported image file formats.

- Raw image files (.001)
- Apple disk image files (.dmg)
- EnCase image files (.E01)
- Advanced Forensic File Format (.aff4)

1. In the toolbar, click **Tools > Hash Image File**.
   The Hash Image File tab appears.

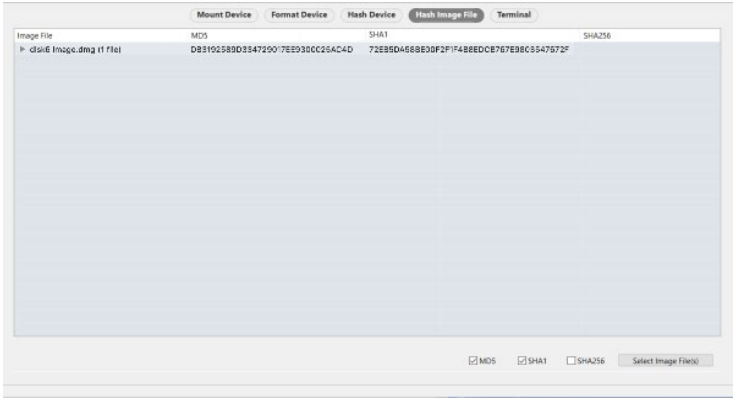


2. Click **Select Image File(s)**.
3. Browse to the image file or files, select it or them, and then click **Open**.
4. The Activity window shows hash progress expressed as hashed data complete, percentage complete, hashing speed (MBs/min), and estimated time remaining. If you select multiple image files and hashes at the same time, the Activity window shows a progress bar for each hash process still in progress.



   To stop the hash process, click **Stop All**. Read the warning message, and then click either **Continue Activity** or **Stop Activity**.

5. When the hash process is complete, selected hash values appear in the Activity window and in the Hash Image File tab in the appropriate column according to hash type.

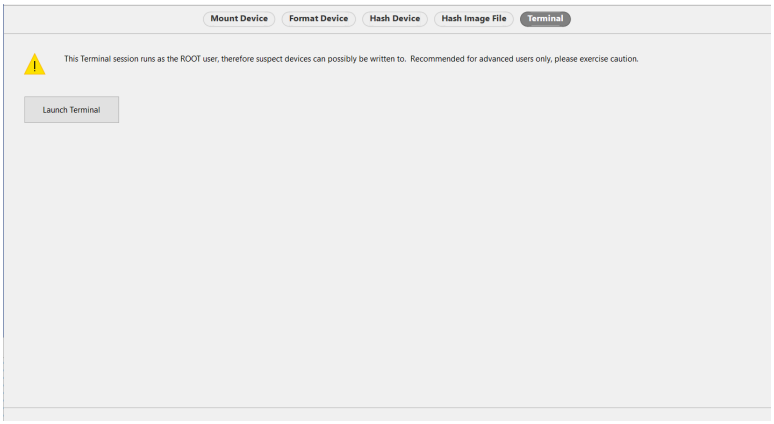


Terminal Tool for macOS

Cellebrite Digital Collector has the iTerm macOS Terminal (command line) emulation application built in. You may run supported Terminal commands directly from within Digital Collector by using this Terminal tool.

Warning: iTerm2 runs with root permissions. Improper use of this tool may result in evidentiary data loss or contamination.

1. In the toolbar, click **Tools > Terminal**.



2. Click **Launch Terminal**.
   A terminal window opens, and a bash shell prompt appears.

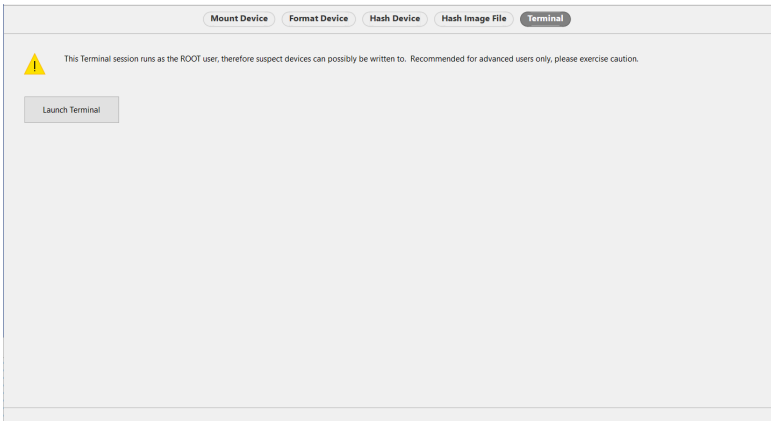
For more information, see http://www.iterm2.com.

Terminal Tool for Windows

You may run supported terminal commands directly from within Cellebrite Digital Collector by using this Terminal tool.

Warning: Windows PowerShell runs with root permissions. Improper use of this tool may result in evidentiary data loss or contamination.

1. In the toolbar, click **Tools > Terminal**.



2. Click **Launch Terminal**.
   A Windows PowerShell window appears with a command prompt.

Frequently Asked Questions

These are some questions frequently asked about Cellebrite Digital Collector.

Why is the DCData partition on the Digital Collector SSD formatted exFAT?

The *DCData* partition on the Digital Collector SSD must have a format that is compatible with both Windows and macOS versions 11 and 12. Apple made changes in Big Sur and Monterey that prevent Digital Collector from writing to NTFS. We had previously discouraged writing macOS data to exFAT; however, our recent testing with macOS 11 and 12 has confirmed that exFAT drivers have improved and are stable for all Digital Collector image formats. Therefore, exFAT is the best format to ensure that data can be written to the *DCData* partition from computers running Windows or macOS versions 11 and 12, whether they are running live or booted from Digital Collector.

When you acquire data from live or booted macOS computers, Digital Collector 3.3 and newer can write to the *DCData* partition when it is formatted as exFAT, APFS, or HFS Plus. Support for writing macOS data to NTFS is only available in the boot environments for Digital Collector versions 3.2 and 3.1 as well as the DC Legacy 2019 boot environment.

When you acquire data from a live Windows computer, Digital Collector 3.3 and newer can write to the *DCData* partition if it is formatted as exFAT or NTFS. However, when a Windows computer is booted from Digital Collector 3.3, data can only be written to the *DCData* partition when it is formatted as exFAT. If you must write to a destination formatted NTFS, you can use your own storage device.

Why is imaging stalling on a Mac laptop?

If the imaging process seems to have stalled on a newer MacBook Pro, MacBook Air, or MacBook with a USB-C port, you should examine the computer time in the Case Details view in Digital Collector. When the battery of a newer Mac laptop is depleted, the computer time defaults to April 1, 1976. An incorrect computer time can cause Digital Collector to stall while imaging. You can adjust it to the current date and time for the imaging process to complete.

1. In the Digital Collector toolbar, click **Case Details**.
2. If the **Current machine time** is not correct, an orange triangle appears.
3. Click **Change**.
4. In the Set System Clock window, adjust the date and time to the current date and time, and then click **Set Time**.

Setting the system time does not affect the data obtained from the source Mac computer, which is attached or mounted as read-only. It does affect the date and time seen in the Digital Collector log files, for example the date and time the image is created.

If the computer time is accurate in the Case Details view but imaging is stalled, try a different cable or a different destination drive.

If imaging is still stalled, contact Technical Support. For more information, see Getting Support.

How do I resolve the License Required message for Digital Collector running live on macOS 10.15 or later?

Changes made by Apple affect how Digital Collector detects its license file on the solid-state device (SSD) when it is connected to a live computer running macOS 10.15 Catalina or later. To run Digital Collector in this situation, you must first grant full disk access to Digital Collector. This requires administrator credentials. If you cannot provide administrator credentials, you can run Digital Collector with restricted permissions.

Grant full disk access

1. In the **Apple** menu, click **System Preferences > Security & Privacy > Privacy**.
2. In the lower left corner of the **Privacy** tab, click the padlock and then provide administrator credentials.
3. In the left pane, click **Full Disk Access**.
4. Either drag the Digital Collector app into the right pane or click **+ (Add)** under the right pane and add the Digital Collector app from the Digital Collector volume of the SSD.

Run with restricted permissions

1. Launch Digital Collector.
2. On the dialog box to enter user credentials, click **Cancel**.
3. On the subsequent dialog box, click **Run Restricted**, and then click **OK**.

Appendix: Changes to Live Computers

In many cases, investigators have no choice but to deal with a live computer, as it may be the only viable option. However, any time we deal with a live computer, changes are unavoidably made to its file system.

Therefore, investigators must know what they are doing and document all their actions so that they can be explained later if necessary. It is impossible to determine every single change that will be made on a live computer; there are too many variables that cannot be accounted for. That said, this is a high-level list of known changes that will be made simply by connecting a Cellebrite Digital Collector device and launching the application on a live computer.

Legend

- NEW New
- ✕ Deleted
- ▬· Content modified
- 🛠 Attributes modified
- ↗ Moved from
- ↘ Moved to

Computers with a Mac Operating System

These are the biggest changes.

- Time stamps for Accessed are updated for every previewed file.
- Running in Restricted mode will likely drop the */private/var/root/* files into the */Users/<USER>/* directory structure.

Changes Made by Connecting a Digital Collector Device

Change	Location
🛠	/private/var/db/diagnostics/Signpost/.tracev3
🛠	/private/var/db/diagnostics/Persist/.tracev3
▬·	/private/var/log/fsck_hfs.log
🛠	/private/var/db/uuidtext/
▬·	/private/var/log/fsck_hfs.log
NEW	/Volumes/DC M Boot
NEW	/Volumes/MacOS App
NEW	/Volumes/DCData
🛠	/private/var/db/reportmemoryexception

Changes Made by Running Digital Collector Live

Change	Location
NEW	/Users/<USER>/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/restorecount.plist
🛠	/private/var/db/diagnostics/Persist/.tracev3
NEW	/private/var/folders/<items>
✕	/private/var/folders/<items>
🛠	/private/var/folders/<items>
↘	/Users/<USER>/Library/Application Support/com.apple.sharedfilelist/
🛠	/Users/<USER>/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.RecentApplications
↗	/Library/Catacomb/<GUID>/.dat.nosync<random value>
↘	/Library/Catacomb/<GUID>/biolockout.cat
▬	/private/var/folders/<temp folders>/com.cellebrite.DigitalCollector/com.apple.metal/3902/libraries.data
▬	/private/var/folders/<temp folders>/com.cellebrite.DigitalCollector/com.apple.metal/Intel(R) UHD Graphics 630/functions.data
NEW	/private/var/root/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/restorecount.plist
🛠	/private/var/db/uuidtext/<temp files>
🛠	/private/var/db/diagnostics/Persist/<integer value>.tracev3
✕	/private/tmp/BBT-BDE12C4F8914
NEW	/private/var/root/Library/Application Support/Cellebrite/DCTemp
✕	/private/var/root/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/restorecount.plist
NEW	/private/var/root/Library/Application Support/Cellebrite/DCTemp/filetaskserr
🛠	/private/var/root/Library/Application Support/Cellebrite/DCTemp/filetaskserr
▬	/private/var/root/Library/Application Support/Cellebrite/DCTemp/filetaskserr
↗	/Users/<USER>/Library/Application Support/com.apple.spotlight/.dat.nosync<random value>
↘	/Users/<USER>/Library/Application Support/com.apple.spotlight/appList.dat
✕	/private/var/root/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/data.data

Change	Location
✕	/private/var/root/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/windows.plist
✕	/private/var/root/Library/Saved Application State/com.cellebrite.DigitalCollector.savedState/window_1.data

Changes Made by Previewing Files

Change	Location
▪	/private/var/folders/<temp folders>/com.apple.QuickLook.thumbnailcache/thumbnails.data
▪	/private/var/folders/<temp folders>/com.apple.QuickLook.thumbnailcache/index.sqlite-shm
▪	/private/var/folders/<temp folders>/com.apple.QuickLook.thumbnailcache/index.sqlite-wal
▪	/private/var/folders/<temp folders>/com.apple.QuickLook.thumbnailcache/index.sqlite
✕	/private/var/folders/<temp folders>/com.apple.QuickLook.thumbnailcache/dirty
NEW	/private/var/root/Library/Application Support/Cellebrite/DCTemp/QLPreview
NEW	/private/var/root/Library/Application Support/Cellebrite/DCTemp/QLPreview/2019 Q4 BvA.xlsx.qlpreview
↗	/private/var/folders/<temp folders>/TemporaryItems/(A Document Being Saved By Quick Look Helper)/Preview.html
↘	/private/var/root/Library/Application Support/Cellebrite/DCTemp/QLPreview/2019 Q4 BvA.xlsx.qlpreview/Preview.html
NEW	/private/var/folders/<temp folders>/com.apple.quicklook.QuickLookUIService/com.apple.quicklook.QuickLookUIService/com.apple.metal/<graphics card>
NEW	/private/var/folders/<temp folders>/com.apple.quicklook.QuickLookUIService/com.apple.quicklook.QuickLookUIService/com.apple.metal/<graphics card>/functions.data
🛠	/private/var/folders/<temp folders>/com.apple.quicklook.QuickLookUIService/com.apple.quicklook.QuickLookUIService/com.apple.metal/<graphics card value>/libraries.maps
NEW	/private/var/folders/<temp folders>/com.apple.quicklook.QuickLookUIService/com.apple.quicklook.QuickLookUIService/com.apple.metal/<graphics card>/functions.maps